No. 15-2560

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION, *et al.*,

Plaintiffs–Appellants,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

On Appeal from the United States District Court
for the District of Maryland
Baltimore Division

JOINT APPENDIX

Patrick Toomey
Jameel Jaffer
Alexander Abdo
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
ptoomey@aclu.org

Counsel for Plaintiffs–Appellants
(additional counsel on reverse)

H. Thomas Byron, III
Catherine H. Dorsey
U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave., NW
Washington, DC 20530
Phone: (202) 616-5367
H.Thomas.Byron@usdoj.gov

Counsel for Defendants–Appellees

Deborah A. Jeon
David R. Rocah
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
jeon@aclu-md.org

Charles S. Sims
David A. Munkittrick
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
csims@proskauer.com

Counsel for Plaintiffs–Appellants

JOINT APPENDIX
TABLE OF CONTENTS

U.S. District Court for the District of Maryland, Docket Sheet, Case No. 1:15-cv-00662-TSE .... JA 1

Plaintiffs' First Amended Complaint (June 22, 2015), ECF No. 72 .... JA 27

Declaration of Dr. Alan Salzberg in support of Defendants' Motion to Dismiss the First Amended Complaint (Aug. 6, 2015), ECF No. 77-2 .... JA 87

Declaration of Robert T. Lee in support of Defendants' Motion to Dismiss the First Amended Complaint (Aug. 6, 2015), ECF No. 77-3 .... JA 101

Transcript of Oral Argument on Defendants' Motion to Dismiss (Sept. 25, 2015) .... JA 122

Memorandum Opinion (Oct. 23, 2015), ECF No. 93 .... JA 174

Order (Oct. 23, 2015), ECF No. 95 .... JA 204

Notice of Appeal (Dec. 15, 2015), ECF No. 96 .... JA 205

APPEAL,CLOSED

U.S. District Court
District of Maryland (Baltimore)
CIVIL DOCKET FOR CASE #: 1:15-cv-00662-TSE

Wikimedia Foundation et al v. National Security Agency/Central Security Service et al
Assigned to: Judge T. S. Ellis
Case in other court: USCA, 15-02560
Cause: 05:706 Judicial Review of Agency Action

Date Filed: 03/10/2015
Date Terminated: 10/23/2015
Jury Demand: None
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: U.S. Government Defendant

Plaintiff

Wikimedia Foundation represented by

Alex Abdo
American Civil Liberties Union Foundation
125 Broad St
18th Floor
New York, NY 10004
2125492517
Fax: 2125492654
Email: aabdo@aclu.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
American Civil Liberties Union Foundation
125 Broad St
18th Floor
New York, NY 10004
2122847305
Fax: 2125492654
Email: agorski@aclu.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693950
Fax: 2129692900
Email: csims@proskauer.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick

Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693226
Fax: 2129692900
Email: dmunkittrick@proskauer.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
ACLU of Maryland
3600 Clipper Mill Rd, #350
Baltimore, MD 21211
14108898555
Fax: 14103667838
Email: rocah@aclu-md.org
ATTORNEY TO BE NOTICED

Jameel Jaffer
American Civil Liberties Union
Foundation
125 Broad St
18th Floor
New York, NY 10004
2125197814
Fax: 2125492654
Email: jjaffer@aclu.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693452
Fax: 2129692900
Email: jbrowning@proskauer.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
American Civil Liberties Union
Foundation
125 Broad St
18th Floor
New York, NY 10004
2125197816
Fax: 2125492654
Email: ptoomey@aclu.org
PRO HAC VICE

ATTORNEY TO BE NOTICED

Deborah A Jeon
American Civil Liberties Union of Maryland Foundation
3600 Clipper Mill Rd Ste 350
Baltimore, MD 21211
14108898555
Fax: 14103667838
Email: jeon@aclu-md.org
ATTORNEY TO BE NOTICED

Plaintiff

National Association of Criminal Defense Attorneys

represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE

ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Human Rights Watch represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Pen American Center represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Global Fund for Women represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski

(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

The Nation Magazine represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)

PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

The Rutherford Institute represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE

ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Washington Office on Latin America represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Amnesty International USA represented by **Alex Abdo**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ashley Marie Gorski
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Charles Sims
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Alexander Munkittrick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Robert Rocah
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

John Browning

(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick Toomey
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Deborah A Jeon
(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

National Security Agency/Central Security Service represented by **James Jordan Gilligan**
United States Department of Justice
20 Massachusetts Ave NW
Rm 6102
Washington, DC 20001
2025143358
Fax: 2026168470
Email: james.gilligan@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
United States Department of Justice
Civil Division Federal Programs Branch
20 Massachusetts Ave NW
Room 5102
Washington, DC 20001
2026168480
Fax: 2026168470
Email: julia.berman@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
United States Department of Justice
20 Massachusetts Ave
Rm 7320
Washington, DC 20530
2023057919
Fax: 2026168470
Email: rodney.patton@usdoj.gov
ATTORNEY TO BE NOTICED

Defendant

Adm. Michael S. Rogers
in his official capacity as Director of the National Security Agency and Chief of the Central Security Service

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Office of the Director of National Intelligence

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

James R. Clapper
in his official capacity as Director of National Intelligence

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Department of Justice

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Eric H. Holder
in his official capacity as Attorney General of the United States
TERMINATED: 06/22/2015

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Loretta E. Lynch
in her official capacity as Attorney General of the United States

represented by **James Jordan Gilligan**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Julia Alexandra Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

CloudFlare
CloudFlare

represented by **Jeffrey Landis**
ZwillGen PLLC
1900 M Street, NW
Suite 250
Washington, DC 20036
12027065203
Fax: 12027065298
Email: jeff@zwillgen.com

Jennifer Stisa Granick

Stanford Center for Internet and Society
559 Nathan Abbot Way
Stanford, CA 94305
6507368675
Email: jennifer@law.stanford.edu
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

The Tor Project, Inc.
The Tor Project, Inc.

represented by **Jeffrey Landis**
(See above for address)

Jennifer Stisa Granick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

RiseUp
RiseUp

represented by **Jeffrey Landis**
(See above for address)

Jennifer Stisa Granick
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

First Amendment Legal Scholars

represented by **Emily Lange Levenson**
Brown, Goldstein & Levy LLP
120 E. Baltimore St
Suite 1700
Baltimore, MD 21202
4109621030
Fax: 4103850869
Email: elevenson@browngold.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joshua R Treem
Brown Goldstein Levy LLP
120 E Baltimore St Ste 1700
Baltimore, MD 21202
14109621030
Fax: 14103850869
Email: jtreem@browngold.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Margot E Kaminski

Moritz College of Law, The Ohio State University
55 W 12th Ave
Columbus, OH 43210
6142922092
Email: kaminski.217@osu.edu
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

The American Booksellers Association represented by **Andrew Gellis Crocker**
Electronic Frontier Foundation
815 Eddy St
San Franscisco, CA 94109
4154369333
Fax: 4154369993
Email: andrew@eff.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
Gohn Hankey Stichel & Berlage, LLP
201 N Charles St Ste 2101
Baltimore, MD 21201
14107529300
Fax: 14107522519
Email: jberlage@ghsllp.com
ATTORNEY TO BE NOTICED

Amicus

American Library Association represented by **Andrew Gellis Crocker**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

Association of Research Libraries represented by **Andrew Gellis Crocker**
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jan Ingham Berlage
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

Freedom to Read Foundation	represented by	**Andrew Gellis Crocker** (See above for address) *PRO HAC VICE* *ATTORNEY TO BE NOTICED* **Jan Ingham Berlage** (See above for address) *ATTORNEY TO BE NOTICED*

Amicus

International Federation of Library Associations and Institutions	represented by	**Andrew Gellis Crocker** (See above for address) *PRO HAC VICE* *ATTORNEY TO BE NOTICED* **Jan Ingham Berlage** (See above for address) *ATTORNEY TO BE NOTICED*

Date Filed	#	Docket Text
03/10/2015	1	COMPLAINT *for Declaratory and Injunctive Relief* against All Defendants (Filing fee $ 400 receipt number 0416-5260730.), filed by The Nation Magazine, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Pen American Center, Wikimedia Foundation, Global Fund for Women, Amnesty International USA. (Attachments: # 1 Civil Cover Sheet, # 2 Summonses)(Jeon, Deborah) (Entered: 03/10/2015)
03/10/2015	2	NOTICE by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation *Summons to U.S. Attorney* (Jeon, Deborah) (Entered: 03/10/2015)
03/10/2015	3	Summons Issued 60 days as to James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers, U.S. Attorney and U.S. Attorney General (bmhs, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	4	MOTION to Appear Pro Hac Vice for Alex Abdo (Filing fee $ 50, receipt number 0416-5262165.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	5	MOTION to Appear Pro Hac Vice for Ashley Gorski (Filing fee $ 50, receipt number 0416-5262203.) by Amnesty International USA, Global Fund for Women,

		Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	6	MOTION to Appear Pro Hac Vice for Jameel Jaffer (Filing fee $ 50, receipt number 0416-5262236.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	7	MOTION to Appear Pro Hac Vice for Patrick Toomey (Filing fee $ 50, receipt number 0416-5262246.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015)
03/10/2015	8	QC NOTICE: 4 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	9	QC NOTICE: 5 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	10	QC NOTICE: 6 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/10/2015	11	QC NOTICE: 7 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015)
03/11/2015	12	CORRECTED MOTION to Appear Pro Hac Vice for Alex Abdo by Amnesty International USA, Global Fund for Women, Human Rights Watch, National

		Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	13	CORRECTED MOTION to Appear Pro Hac Vice for Ashley Gorski by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	14	PAPERLESS ORDER granting 12 Corrected Motion to Appear Pro Hac Vice on behalf of Alex Abdo. Directing attorney Alex Abdo to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	15	PAPERLESS ORDER granting 13 Corrected Motion to Appear Pro Hac Vice on behalf of Ashley Gorski. Directing attorney Ashley Gorski to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	16	CORRECTED MOTION to Appear Pro Hac Vice for Jameel Jaffer by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	17	CORRECTED MOTION to Appear Pro Hac Vice for Patrick Toomey by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015)
03/11/2015	18	MOTION to Appear Pro Hac Vice for Charles Sims (Filing fee $ 50, receipt number 0416-5265356.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015)
03/11/2015	19	MOTION to Appear Pro Hac Vice for David Munkittrick (Filing fee $ 50, receipt number 0416-5265372.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015)
03/11/2015	20	MOTION to Appear Pro Hac Vice for John Browning (Filing fee $ 50, receipt number 0416-5265384.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington

		Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015)
03/11/2015	21	PAPERLESS ORDER granting 16 Corrected Motion to Appear Pro Hac Vice on behalf of Jameel Jaffer. Directing attorney Jameel Jaffer to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	22	PAPERLESS ORDER granting 17 Corrected Motion to Appear Pro Hac Vice on behalf of Patrick Toomey. Directing attorney Patrick Toomey to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	23	PAPERLESS ORDER granting 18 Motion to Appear Pro Hac Vice on behalf of Charles Sims. Directing attorney Charles Sims to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	24	PAPERLESS ORDER granting 19 Motion to Appear Pro Hac Vice on behalf of David Munkittrick. Directing attorney David Munkittrick to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	25	PAPERLESS ORDER granting 20 Motion to Appear Pro Hac Vice on behalf of John Browning. Directing attorney John Browning to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015)
03/11/2015	26	Local Rule 103.3 Disclosure Statement by Amnesty International USA. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	27	Local Rule 103.3 Disclosure Statement by Global Fund for Women. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	28	Local Rule 103.3 Disclosure Statement by Human Rights Watch. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	29	Local Rule 103.3 Disclosure Statement by National Association of Criminal Defense Attorneys identifying Other Affiliate Foundation for Criminal Justice for National Association of Criminal Defense Attorneys.. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	30	Local Rule 103.3 Disclosure Statement by Pen American Center. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	31	Local Rule 103.3 Disclosure Statement by The Rutherford Institute. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	32	Local Rule 103.3 Disclosure Statement by The Nation Magazine. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	33	Local Rule 103.3 Disclosure Statement by Wikimedia Foundation. (Rocah, David) (Entered: 03/11/2015)
03/11/2015	34	Local Rule 103.3 Disclosure Statement by Washington Office on Latin America.

		(Rocah, David) (Entered: 03/11/2015)
03/17/2015	35	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on United States Attorney for the District of Maryland on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	36	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Office of the Director of National Intelligence on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	37	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on National Security Agency / Central Security Service on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	38	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Department of Justice on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	39	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Adm. Michael S. Rogers on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	40	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Director of National Intelligence James R. Clapper on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	41	(FILED IN ERROR) AFFIDAVIT of Service for Summons served on Attorney General Eric H. Holder, Jr. on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey,

		Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015)
03/17/2015	42	QC NOTICE: 35 Affidavit of Service filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA was filed incorrectly. ***Incorrect event was selected. Please refile using the event under Service of Process - Summons Returned Executed as to USA AND case caption and case number are missing. It has been noted as FILED IN ERROR, and the document link has been disabled.* (bmhs, Deputy Clerk) (Entered: 03/17/2015)
03/17/2015	43	QC NOTICE: 36 37 38 39 40 41 Affidavits of Service filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA were filed incorrectly. ***Case caption and case number are missing. It has been noted as FILED IN ERROR, and the document link has been disabled.* (bmhs, Deputy Clerk) (Entered: 03/17/2015)
03/17/2015	44	SUMMONS Returned Executed by The Nation Magazine, Amnesty International USA, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Wikimedia Foundation, Pen American Center, Global Fund for Women. James R. Clapper served on 3/10/2015, answer due 5/11/2015; Department of Justice served on 3/10/2015, answer due 5/11/2015; Eric H. Holder served on 3/10/2015, answer due 5/11/2015; National Security Agency/Central Security Service served on 3/10/2015, answer due 5/11/2015; Office of the Director of National Intelligence served on 3/10/2015, answer due 5/11/2015; Michael S. Rogers served on 3/10/2015, answer due 5/11/2015. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	45	AFFIDAVIT of Service for Summons served on Office of the Director of National Intelligence on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	46	AFFIDAVIT of Service for Summons served on National Security Agency / Central Security Service on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	47	AFFIDAVIT of Service for Summons served on Director of National Intelligence James R. Clapper on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)

03/17/2015	48	AFFIDAVIT of Service for Summons served on Department of Justice on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	49	AFFIDAVIT of Service for Summons served on Adm. Michael S. Rogers on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/17/2015	50	AFFIDAVIT of Service for Summons served on Attorney General Eric H. Holder, Jr. on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015)
03/19/2015	51	NOTICE of Appearance by James Jordan Gilligan on behalf of All Defendants (Gilligan, James) (Entered: 03/19/2015)
03/23/2015	52	NOTICE of Appearance by Rodney Patton on behalf of James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Patton, Rodney) (Entered: 03/23/2015)
03/24/2015	53	NOTICE of Appearance by Julia Alexandra Berman on behalf of All Defendants (Berman, Julia) (Entered: 03/24/2015)
03/26/2015		Case reassigned to Judge T. S. Ellis. Judge Richard D Bennett no longer assigned to the case. (cags, Deputy Clerk) (Entered: 03/26/2015)
04/24/2015	54	MOTION to Set a Status Conference by James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 5/11/2015 (Attachments: # 1 Exhibit 1, # 2 Text of Proposed Order)(Berman, Julia) (Entered: 04/24/2015)
04/28/2015	55	RESPONSE to Motion re 54 MOTION to Set a Status Conference filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Replies due by 5/15/2015. (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 04/28/2015)
04/30/2015	56	ORDER granting 54 Defendants' Motion to set a status conference; and scheduling a status conference for 3:30 p.m. on Wednesday, May 13, 2015. Signed by Judge T. S. Ellis on 4/30/2015. (bmhs, Deputy Clerk) (Entered: 04/30/2015)
05/06/2015	57	Correspondence re: Request Pursuant to D. Md. Local Rule 101.1(b)(i) for May

		13, 2015 Status Conference (Toomey, Patrick) (Entered: 05/06/2015)
05/11/2015	58	ORDER granting 57 Plaintiffs' Letter Motion. Signed by Judge T. S. Ellis on 5/11/15. (bmhs, Deputy Clerk) (Entered: 05/11/2015)
05/12/2015	59	PAPERLESS ORDER, for good cause, it is hereby ORDERED that the status conference scheduled to be heard at the Greenbelt Courthouse at 3:30 p.m. on Wednesday, May 13, 2015, is CANCELED. Instead, a telephone conference is SCHEDULED for the same date and time (3:30 p.m. on Wednesday, May 13, 2015). In this regard, all participating counsel are DIRECTED first to conference themselves together on one phone line and then to call Chambers at (703) 299-2114 to commence the conference call. Signed by Judge T. S. Ellis on 5/12/2015. (bmhs, Deputy Clerk) (Entered: 05/12/2015)
05/14/2015	60	Telephone Conference held on 5/14/2015 before Judge T. S. Ellis. (bmhs, Deputy Clerk) (Entered: 05/15/2015)
05/14/2015	61	ORDER directing parties to comply with the briefing and argument schedule. Signed by Judge T. S. Ellis on 5/13/2015. (bmhs, Deputy Clerk) (Entered: 05/15/2015)
05/27/2015	62	MOTION to Set a Date for the Filing of Amicus Briefs by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/15/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 05/27/2015)
05/28/2015	63	ORDER denying 62 Motion to Set a Date for the Filing of Amicus Briefs. Signed by Judge T. S. Ellis on 5/28/2015. (bmhs, Deputy Clerk) (Entered: 05/28/2015)
05/29/2015	64	Joint MOTION to Conduct Hearings in Alexandria, Virginia by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/15/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 05/29/2015)
05/29/2015	65	ORDER granting 64 Joint Motion to Conduct Hearings in Alexandria, Virginia. Signed by Judge T. S. Ellis on 5/29/2015. (bmhs, Deputy Clerk) (Entered: 05/29/2015)
05/29/2015	66	MOTION to Dismiss for Lack of Jurisdiction *Under Rule 12(b)(1)* by James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 6/15/2015 (Attachments: # 1 Memorandum of Law in Support of Motion to Dismiss, # 2 Text of Proposed Order, # 3 Exhibit Exhibit List, # 4 Exhibit Exhibit 1, # 5 Exhibit Exhibit 2, # 6 Exhibit Exhibit 3, # 7 Exhibit Exhibit 4A, # 8 Exhibit Exhibit 4B, # 9 Exhibit Exhibit 4C, # 10 Exhibit Exhibit 4D, # 11 Exhibit Exhibit 5, # 12 Exhibit Exhibit 6)(Patton, Rodney) (Entered: 05/29/2015)
06/12/2015	67	Joint MOTION to Amend the Briefing Schedule by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal

		Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/29/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 06/12/2015)
06/12/2015	68	ORDER granting 67 Joint Motion to Amend the Briefing Scheduling governing Defendants' Motion to Dismiss; and postponing the oral argument on Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 6/12/2015. (bmhs, Deputy Clerk) (Entered: 06/15/2015)
06/12/2015	69	ORDER amending the briefing schedule. Signed by Judge T. S. Ellis on 6/12/2015. (bmhs, Deputy Clerk) (Entered: 06/15/2015)
06/19/2015	70	MOTION to Amend/Correct 1 Complaint, by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 7/9/2015 (Attachments: # 1 First Amended Complaint, # 2 First Amended Complaint - Redline, # 3 Text of Proposed Order)(Toomey, Patrick) (Entered: 06/19/2015)
06/22/2015	71	ORDER granting 70 Plaintiffs' Motion to Amend the Complaint; and denying as moot 66 Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 6/22/2015. (bmhs, Deputy Clerk) (Entered: 06/22/2015)
06/22/2015	72	AMENDED COMPLAINT against James R. Clapper, Department of Justice, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers, Loretta E. Lynch filed by The Nation Magazine, Amnesty International USA, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Wikimedia Foundation, Pen American Center, Global Fund for Women. (Attachments: # 1 Red Line Complaint)(bmhs, Deputy Clerk) (Entered: 06/22/2015)
06/27/2015	73	Consent MOTION for Extension of Time by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 7/16/2015 (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 06/27/2015)
06/29/2015	74	ORDER granting 73 Consent Motion for Extension of Time. Signed by Judge T. S. Ellis on 6/29/2015. (bmhs, Deputy Clerk) (Entered: 06/29/2015)
07/31/2015	75	MOTION to Appear Pro Hac Vice for Jennifer Stisa Granick (Filing fee $ 50, receipt number 0416-5525629.) by CloudFlare, The Tor Project, Inc., RiseUp (Landis, Jeffrey) (Entered: 07/31/2015)
08/03/2015	76	PAPERLESS ORDER granting 75 Motion to Appear Pro Hac Vice on behalf of Jennifer Stisa Granick. Directing attorney Jennifer Stisa Granick to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 8/3/2015. (bu, Deputy Clerk) (Entered: 08/03/2015)
08/06/2015	77	MOTION to Dismiss for Lack of Jurisdiction by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service,

		Office of the Director of National Intelligence, Michael S. Rogers Responses due by 8/24/2015 (Attachments: # 1 (Memorandum in Support), # 2 Affidavit (Salzberg Declaration), # 3 Affidavit (Lee Declaration Part 1), # 4 Affidavit (Lee Declaration Part 2), # 5 Affidavit (Lee Declaration Part 3), # 6 Affidavit (Lee Declaration Part 4), # 7 Affidavit (Lee Declaration Part 5), # 8 Exhibit 1, # 9 Exhibit 2, # 10 Exhibit 3, # 11 Exhibit 4, # 12 Exhibit 5, # 13 Exhibit 6, # 14 Exhibit 7, # 15 Exhibit 8, # 16 Exhibit 9, # 17 (Index of Exhibits), # 18 Text of Proposed Order)(Gilligan, James) (Entered: 08/06/2015)
09/03/2015	78	NOTICE of Appearance by Joshua R Treem on behalf of First Amendment Legal Scholars (Treem, Joshua) (Entered: 09/03/2015)
09/03/2015	79	NOTICE of Appearance by Emily Lange Levenson on behalf of First Amendment Legal Scholars (Levenson, Emily) (Entered: 09/03/2015)
09/03/2015	80	MOTION to Appear Pro Hac Vice (Filing fee $ 50, receipt number 0416-5581832.) by First Amendment Legal Scholars (Treem, Joshua) (Entered: 09/03/2015)
09/03/2015	81	NOTICE of Appearance by Jan Ingham Berlage on behalf of The American Booksellers Association, American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions (Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	82	MOTION for Leave to File *to File Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss* by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association Responses due by 9/21/2015 (Attachments: # 1 Brief in Opposition to Defendants' Motion to Dismiss)(Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	83	MOTION to Appear Pro Hac Vice for Andrew Crocker (Filing fee $ 50, receipt number 0416-5582368.) by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association (Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	84	NOTICE by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association re 81 Notice of Appearance, 82 MOTION for Leave to File *to File Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss*, 83 MOTION to Appear Pro Hac Vice for Andrew Crocker (Filing fee $ 50, receipt number 0416-5582368.) *of Service* (Berlage, Jan) (Entered: 09/03/2015)
09/03/2015	85	MOTION for Leave to File *Brief of Amicus Curiae* by First Amendment Legal Scholars Responses due by 9/21/2015 (Attachments: # 1 Brief of Amicus Curiae First Amendment Legal Scholars, # 2 Text of Proposed Order)(Treem, Joshua) (Entered: 09/03/2015)
09/03/2015	86	RESPONSE in Opposition re 77 MOTION to Dismiss for Lack of Jurisdiction filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American

		Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Replies due by 9/21/2015. (Toomey, Patrick) (Entered: 09/03/2015)
09/09/2015	87	PAPERLESS ORDER granting 80 Motion to Appear Pro Hac Vice on behalf of Margot E Kaminski. Directing attorney Margot E Kaminski to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 9/9/2015. (srd, Intern) (Entered: 09/09/2015)
09/09/2015	88	PAPERLESS ORDER granting 83 Motion to Appear Pro Hac Vice on behalf of Andrew Crocker. Directing attorney Andrew Crocker to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 9/9/2015. (srd, Intern) (Entered: 09/09/2015)
09/17/2015	89	REPLY to Response to Motion re 77 MOTION to Dismiss for Lack of Jurisdiction filed by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit 1)(Gilligan, James) (Entered: 09/17/2015)
09/25/2015	90	Status Conference held on 9/25/2015 before Judge T. S. Ellis. (Court Reporter: M. Pham) (bmhs, Deputy Clerk) (Entered: 09/28/2015)
09/25/2015	91	ORDER taking under advisment 77 Defendant's MOTION to Dismiss for Lack of Jurisdiction. Signed by Judge T. S. Ellis on 9/25/2015. (bmhs, Deputy Clerk) (Entered: 09/28/2015)
10/22/2015	92	MOTION to Withdraw as Attorney by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 11/9/2015 (Attachments: # 1 Text of Proposed Order)(Rocah, David) (Entered: 10/22/2015)
10/23/2015	93	MEMORANDUM OPINION. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015)
10/23/2015	94	ORDER granting 82 85 amici curiae's Motions for Leave to File amicus curiae briefs. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015)
10/23/2015	95	ORDER granting 77 Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015)
12/15/2015	96	NOTICE OF APPEAL as to 95 Order on Motion to Dismiss/Lack of Jurisdiction by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Filing fee $ 505, receipt number 0416-5759619. (Toomey, Patrick) (Entered: 12/15/2015)
12/17/2015	97	Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals re 96 Notice of Appeal. IMPORTANT NOTICE: To access forms which you are required to file with the United States Court of Appeals for the Fourth Circuit please go to http://www.ca4.uscourts.gov and click on Forms & Notices. (sls,

		Deputy Clerk) (Entered: 12/17/2015)
12/18/2015	98	USCA Case Number 15-2560 for 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA. Case Manager - RJ Warren (ko, Deputy Clerk) (Entered: 12/18/2015)
12/29/2015	99	(ELECTRONICALLY FILED IN ERROR)TRANSCRIPT REQUEST by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation for proceedings held on September 25, 2015 before Judge T.S. Ellis, III.. (Toomey, Patrick) Modified on 12/29/2015 (slss, Deputy Clerk). (Entered: 12/29/2015)
01/04/2016	100	NOTICE OF FILING OF OFFICIAL TRANSCRIPT for dates of September 25, 2015, before Judge T.S. Ellis, III, re 96 Notice of Appeal, Court Reporter/Transcriber Michael A. Rodriquez, Telephone number 301-213-4913. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Does this satisfy all appellate orders for this reporter? - Y. Redaction Request due 1/25/2016. Redacted Transcript Deadline set for 2/4/2016. Release of Transcript Restriction set for 4/4/2016. (jbps, Deputy Clerk) (Entered: 01/04/2016)

PACER Service Center

Transaction Receipt

01/26/2016 16:03:24

PACER Login:	agorski12:4393661:4375869	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	1:15-cv-00662-TSE
Billable Pages:	24	**Cost:**	2.40

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION 149 New Montgomery Street, 6th Floor San Francisco, CA 94105; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS 1660 L Street, NW, 12th Floor Washington, DC 20036; HUMAN RIGHTS WATCH 350 Fifth Avenue, 34th Floor New York, NY 10118; AMNESTY INTERNATIONAL USA 5 Pennsylvania Plaza, 16th Floor New York, NY 10001; PEN AMERICAN CENTER 588 Broadway, Suite 303 New York, NY 10012; GLOBAL FUND FOR WOMEN 222 Sutter Street, Suite 500 San Francisco, CA 94108; THE NATION MAGAZINE 33 Irving Place, 8th Floor New York, NY 10003; THE RUTHERFORD INSTITUTE P.O. Box 7482 Charlottesville, VA 22906; WASHINGTON OFFICE ON LATIN AMERICA 1666 Connecticut Avenue, NW, Suite 400 Washington, DC 20009, *Plaintiffs*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE	**FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF** Civil Action No. 15-cv-00662-TSE Hon. T. S. Ellis, III

9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service, National Security Agency / Central Security Service
9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Washington, DC 20511;

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence,
Office of the Director of National Intelligence
Washington, DC 20511;

DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, NW
Washington, DC 20530;

LORETTA E. LYNCH, in her official capacity as Attorney General of the United States,
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530,

Defendants.

Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)
csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

June 19, 2015

FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. The NSA conducts this surveillance, called "Upstream" surveillance, by tapping directly into the internet backbone inside the United States—the network of high-capacity cables, switches, and routers that today carry vast numbers of Americans' communications with each other and with the rest of the world. In the course of this surveillance, the NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms. The surveillance exceeds the scope of the authority that Congress provided in the FISA Amendments Act of 2008 ("FAA") and violates the First and Fourth Amendments. Because it is predicated on programmatic surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy, the surveillance also violates Article III of the Constitution.

2. Plaintiffs are educational, legal, human rights, and media organizations that collectively engage in more than a trillion sensitive international communications over the internet each year. Plaintiffs communicate with, among many others, journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses. Plaintiff Wikimedia Foundation communicates with the hundreds of millions of individuals who visit Wikipedia webpages to read or contribute to the vast repository of human knowledge that Wikimedia maintains online. The ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of

Case 1:15-cv-00662-TSE Document 72 Filed 08/21/15 Page 5 of 60

the Plaintiffs' work. The challenged surveillance violates Plaintiffs' privacy and undermines their ability to carry out activities crucial to their missions.

3. Plaintiffs respectfully request that the Court declare the government's Upstream surveillance to be unlawful; enjoin the government from continuing to conduct Upstream surveillance of Plaintiffs' communications; and require the government to purge from its databases all of Plaintiffs' communications that Upstream surveillance has already allowed the government to obtain.

JURISDICTION AND VENUE

4. This case arises under the Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the Constitution and 28 U.S.C. § 1331. The Court also has jurisdiction under the Administrative Procedure Act, 5 U.S.C. § 702. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412.

5. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (e)(1).

PLAINTIFFS

6. Wikimedia Foundation ("Wikimedia") is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the internet. Wikimedia's mission is to empower people around the world to collect and develop free educational content. Wikimedia does this by developing and maintaining "wiki"-based projects, and by providing the full contents of those projects to individuals around the world free of charge. Wikimedia sues on its own behalf and on behalf of its staff and users.

7. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL advocates for rational and humane criminal justice policies at all levels of federal, state, and local government, and seeks to foster the integrity, independence, and expertise of the criminal defense profession. NACDL sues on its own behalf and on behalf of its members.

8. Human Rights Watch ("HRW") is a non-profit, non-governmental human rights organization headquartered in New York City with offices around the world. It reports on abuses in all regions of the globe and advocates for the protection of human rights. HRW researchers conduct fact-finding investigations into human rights abuses in over 90 countries and publish their findings in hundreds of reports, multi-media products, and other documents every year, as well as through social media accounts. HRW sues on its own behalf and on behalf of its staff.

9. Amnesty International USA ("AIUSA"), headquartered in New York City, is the largest country section of Amnesty International, with hundreds of thousands of members and other supporters who work for human rights, including through national online networks, high schools, colleges, and community groups. AIUSA sues on its own behalf and on behalf of its staff and members.

10. PEN American Center ("PEN") is a human rights and literary association based in New York City. Committed to the advancement of literature and the unimpeded flow of ideas and information, PEN fights for freedom of expression; advocates on behalf of writers harassed, imprisoned, and sometimes killed for their views; and fosters international exchanges, dialogues, discussions, and debates. PEN sues on its own behalf and on behalf of its staff and members.

11. Global Fund for Women ("GFW") is a non-profit grantmaking foundation based in San Francisco, California, and New York City. GFW advances women's human rights worldwide by providing funds to women-led organizations that promote the economic security, health, safety, education, and leadership of women and girls. GFW sues on its own behalf and on behalf of its staff.

12. The Nation Magazine ("The Nation"), which is published by The Nation Company, LLC, and based in New York City, is America's oldest weekly magazine of opinion, news, and culture. It serves as a critical, independent voice in American journalism, exposing abuses of power through its investigative reporting, analysis, and commentary. In recent years, The Nation's journalists have reported on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities in China and elsewhere in East Asia, and conflicts in Africa and Latin America. The Nation sues on behalf of itself, its staff, and certain of its contributing journalists.

13. The Rutherford Institute ("Rutherford") is a civil liberties organization based in Charlottesville, Virginia, committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments. Rutherford sues on its own behalf and on behalf of its staff.

14. The Washington Office on Latin America ("WOLA") is a non-profit, non-governmental organization based in Washington, D.C., that conducts research, advocacy, and education designed to advance human rights and social justice in the Americas. WOLA sues on its own behalf and on behalf of its staff.

DEFENDANTS

15. Defendant National Security Agency / Central Security Service ("NSA"), headquartered in Fort Meade, Maryland, is the agency of the United States government responsible for conducting the surveillance challenged in this case.

16. Defendant Adm. Michael S. Rogers is the Director of the NSA and the Chief of the Central Security Service. Defendant Rogers is sued in his official capacity.

17. Defendant Office of the Director of National Intelligence ("ODNI") is the agency of the United States government responsible for directing and coordinating the activities of the intelligence community, including the NSA.

18. Defendant James R. Clapper is the Director of National Intelligence ("DNI"). Together with the Attorney General, the DNI authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Clapper is sued in his official capacity.

19. Defendant Department of Justice ("DOJ") is one of the agencies of the United States government responsible for authorizing and overseeing surveillance conducted pursuant to the FAA, including Upstream surveillance.

20. Defendant Loretta E. Lynch is the Attorney General of the United States. Together with the DNI, the Attorney General authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Lynch is sued in her official capacity.

LEGAL AND FACTUAL BACKGROUND

The Foreign Intelligence Surveillance Act

21. In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to govern surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered the court to grant or deny government applications for surveillance orders in certain foreign intelligence investigations.

22. Congress enacted FISA after years of in-depth congressional investigation by the committees chaired by Senator Frank Church and Representative Otis Pike, which revealed that the Executive Branch had engaged in widespread warrantless surveillance of United States citizens—including journalists, activists, and members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security."

23. Congress has amended FISA multiple times since 1978.

24. Prior to 2007, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. To obtain a traditional FISA order, the government was required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—often a telephone line or email account—to be monitored. The government was also required to certify that a "significant purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B).

25. The FISC could issue such an order only if it found, among other things, that there was probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the

electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2)(A)–(B).

26. The framework established by FISA remains in effect today, but it has been modified by the FAA to permit the acquisition of U.S. citizens' and residents' international communications without probable cause or individualized suspicion, as described below.

The Warrantless Wiretapping Program

27. On October 4, 2001, President George W. Bush secretly authorized the NSA to conduct a program of warrantless electronic surveillance inside the United States. This program, which was known as the President's Surveillance Program ("PSP"), was reauthorized repeatedly by President Bush between 2001 and 2007.

28. According to public statements by senior government officials, the PSP involved the warrantless interception of emails and telephone calls that originated or terminated inside the U.S. According to then-Attorney General Alberto Gonzales and then-NSA Director General Michael Hayden, NSA "shift supervisors" initiated surveillance when in their judgment there was a "reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."

29. On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISC had "issued orders authorizing the Government to target for collection international communications into or out of the United States where there [was] probable cause to believe that one of the communicants [was] a member or agent of al Qaeda or an associated terrorist organization." The Attorney General further stated that "[a]s a result of

these orders, any electronic surveillance that was occurring" as part of the PSP would thereafter "be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

30. In April 2007, when the government sought reauthorization of the FISC's previous orders, a different judge of the FISC determined that key elements of the government's request were incompatible with FISA. Following the FISC's refusal to renew certain portions of its January 2007 orders, executive-branch officials appealed to Congress to amend the statute.

The Protect America Act

31. Congress enacted the Protect America Act ("PAA") in August 2007. The PAA expanded the executive's surveillance authority and provided legislative sanction for surveillance that the President had previously been conducting under the PSP. Because of a "sunset" provision, the amendments to FISA made by the PAA expired on February 17, 2008.

The FISA Amendments Act

32. President Bush signed the FISA Amendments Act ("FAA") into law on July 10, 2008. The FAA radically revised the FISA regime that had been in place since 1978 by authorizing the acquisition without individualized suspicion of a wide swath of communications, including U.S. persons' international communications, from companies inside the United States.[1]

33. In particular, the FAA allows the Attorney General and Director of National Intelligence to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence

---

[1] Plaintiffs use the term "international" to describe communications that either originate or terminate outside the United States, but not both—*i.e.*, communications that are foreign at one end.

Case 1:15-cv-00662-TSE Document 70 Filed 06/22/15 Page 12 of 60

information." 50 U.S.C. § 1881a(a). The statute requires the Attorney General, in consultation with the Director of National Intelligence, to adopt "targeting procedures" and "minimization procedures," *id.* § 1881a(d)–(e), that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted.

34. The FISC's role in overseeing the government's surveillance under the statute consists principally of reviewing these general procedures. The FISC never reviews or approves the government's individual surveillance targets or the facilities it intends to monitor. Rather, when the government wishes to conduct surveillance under the statute, it must certify to the FISC that the court has approved its targeting and minimization procedures or that it will shortly submit such procedures for the FISC's approval. *See id.* § 1881a(g), (i). If the government so certifies, the FISC authorizes the government's surveillance for up to a year at a time. A single such order may result in the acquisition of the communications of thousands of individuals.

35. The effect of the FAA is to give the government sweeping authority to conduct warrantless surveillance of U.S. persons' international communications. While the statute prohibits the government from intentionally *targeting* U.S. persons, it authorizes the government to acquire U.S. persons' communications with the foreigners whom the NSA chooses to target. Moreover the statute does not meaningfully restrict *which* foreigners the government may target. The statute does not require the government to make any finding—let alone demonstrate probable cause to the FISC—that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. The government may target any person for surveillance if it has a reasonable belief that she is a foreigner outside the United States who is likely to communicate "foreign intelligence information"—a term that is

defined so broadly as to encompass virtually any information relating to the foreign affairs of the United States. *Id.* §§ 1881a(a), 1801(e). The government may target corporations and associations under the same standard.

36. Thus, though the FAA is nominally concerned with the surveillance of individuals and groups outside the United States, it has far-reaching implications for U.S. persons' privacy. The targets of FAA surveillance may include journalists, academic researchers, human rights defenders, aid workers, business persons, and others who are not suspected of any wrongdoing. In the course of FAA surveillance, the government may acquire the communications of U.S. citizens and residents with all these persons.

THE GOVERNMENT'S IMPLEMENTATION OF THE FAA

37. The government has implemented the FAA expansively, with significant consequences for Americans' privacy. The Director of National Intelligence has reported that, in 2014, the government relied on the FAA to target 92,707 individuals, groups, or organizations for surveillance under a single court order. According to the FISC, the government gathered 250 million internet communications under the FAA in 2011 alone—at a time when the NSA had far fewer targets than it has today. Moreover, as described below, that figure does not reflect the far greater number of communications that the NSA searched for references to its targets before discarding them. Intelligence officials have declined to determine, or even estimate, how many of the communications intercepted under the FAA are to, from, or about U.S. citizens or residents. However, opinions issued by the FISC, reports by the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board, and media accounts indicate that FAA

surveillance results in the wide-ranging and persistent interception of U.S. persons' communications.

38. In at least one respect, the government has engaged in surveillance that exceeds even the broad authority that Congress granted in the FAA. As described below, the government has interpreted the FAA to allow it to intercept, copy, and review essentially everyone's internet communications in order to search for identifiers associated with its targets. This intrusive and far-reaching practice has no basis in the statute. The statute authorizes surveillance only of *targets'* communications; it does not authorize surveillance of everyone.

Upstream Surveillance of Internet Communications

39. The government conducts at least two kinds of surveillance under the FAA. Under a program called "PRISM," the government obtains stored and real-time communications directly from U.S. companies—such as Google, Yahoo, Facebook, and Microsoft—that provide communications services to targeted accounts.

40. This case concerns a second form of surveillance, called Upstream. Upstream surveillance involves the NSA's seizing and searching the internet communications of U.S. citizens and residents en masse as those communications travel across the internet "backbone" in the United States. The internet backbone is the network of high-capacity cables, switches, and routers that facilitates both domestic and international communication via the internet.

Background: Internet Communications

41. The internet is a global network of networks. It allows machines of different types to communicate with each other through a set of intermediating networks. At its most basic level, it consists of (1) computers and the connections between them, (2) the

communications transmitted to, by, or through those computers and connections, and (3) the rules that direct the flow of these communications.

42. All communications on the internet are broken into "packets"—discrete chunks of information that are relatively small. The packets are sent from machine to machine (and network to network) and may traverse a variety of physical circuits connecting different machines before reaching their destination. Once the packets that make up a particular communication reach their final destination, they are reassembled so that the recipient can "read" the message being sent—whether an email, a webpage, or a video.

43. Internet packets can be thought of in layers. Although computer scientists describe these layers differently depending on the context, there are three layers relevant here:

- **The Networking Layer:** The Networking Layer of a packet is like an address block on an envelope. It contains, among other things, the packet's source and destination addresses. On the internet, addresses are represented as numeric strings known as Internet Protocol ("IP") addresses. To send a packet from one IP address to another, a computer on the internet creates a packet, addresses the packet with the source and destination IP addresses, and then transmits the packet to a neighboring computer that is closer to the destination. That computer then transmits the packet to another that is closer still to the destination. This process continues until the packet reaches its destination.

- **The Transport Layer:** The Transport Layer of a packet contains information that allows it to be grouped with other packets that are part of the same session or class of communication. For example, a packet sent using the most common Transport Layer protocol (the Transmission Control Protocol ("TCP")) contains, among other things, (1) a sequence number, which allows the recipient to reassemble the packets of a communication in order, and (2) source and destination "ports," which are, in effect, internal addresses used by the sending and receiving computers.

- **The Application Layer:** The Application Layer of a packet is akin to the inside of an envelope—it contains the actual content of the communications being transmitted. If the content is too large to fit into a single packet, then the Application Layers of several different packets would need to be reassembled in order for the recipient to be able to read or interpret the communication. For example, HTTP is the Application Layer protocol used to transmit webpages. Because most websites exceed the size of a single internet packet, their contents are transmitted in a series of HTTP packets that must be reassembled before display. Other common Application Layer protocols that, like

HTTP, contain text-searchable data are SMTP (for the sending of email), IMAP and POP (for the receiving of email), and DNS (which allows computers to learn a website's IP address based on its domain name).

44. In some cases, internet packets stay on a single network (e.g., two machines in the same office talking to each other), but in other cases, the packets may traverse dozens of intermediate networks before reaching their destination. The network path can change radically and dynamically as devices and connections are added or removed from the network.

45. Often, there are multiple routes that an internet packet could follow to reach its destination. Some connected networks may be faster, cheaper, or have a wider reach. Moreover, many high-bandwidth connections route traffic based on complex contractual arrangements, which take into account factors such as cost, the type of traffic, or the balance between inbound and outbound traffic. Networks that are strategically well-connected and have high bandwidth are likely to be used for transit by packets coming from other, less-well-connected networks. These more strategically connected networks, which often link large metropolitan areas, are collectively referred to as the internet "backbone." The overwhelming majority of backbone links are fiber-optic cables, because fiber-optic connections have high bandwidth and can distribute data over long distances.

46. The internet backbone includes the approximately 49 international submarine cables that carry internet communications into and out of the United States and that land at approximately 43 different points within the country. The vast majority of international traffic into and out of the United States traverses this limited number of submarine cables.

Upstream Surveillance

47. The NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers on the internet backbone inside the United

States. These access points are controlled by the country's largest telecommunications providers, including Verizon Communications, Inc. and AT&T, Inc. In some or all instances, aspects of Upstream surveillance may be conducted by the telecommunications providers on the government's behalf.

48. Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic. With the assistance of telecommunications providers, the NSA intercepts a wide variety of internet communications, including emails, instant messages, webpages, voice calls, and video chats. It copies and reviews substantially all international emails and other "text-based" communications—*i.e.*, those whose content includes searchable text.

49. More specifically, Upstream surveillance encompasses the following processes, some of which are implemented by telecommunications providers acting at the NSA's direction:

- **Copying.** Using surveillance devices installed at key access points along the internet backbone, the NSA makes a copy of substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. The copied traffic includes email, internet-messaging communications, web-browsing content, and search-engine queries.

- **Filtering.** The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, using IP filters for instance, while preserving international communications. The NSA's filtering out of domestic communications is incomplete, however, for multiple reasons. Among them, the NSA does not eliminate bundles of domestic and international communications that transit the internet backbone together. Nor does it eliminate domestic communications that happen to be routed abroad.

- **Content Review.** The NSA reviews the copied communications—including their full content—for instances of its search terms. The search terms, called "selectors," include email addresses, phone numbers, IP addresses, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets. Again, the NSA's targets are not limited to suspected foreign agents and terrorists, nor are its selectors limited to individual email addresses. The NSA may monitor or "task" selectors used by large groups of people who are not suspected of any wrongdoing—such as the IP addresses of computer servers used by hundreds of different people.

- **Retention and Use.** The NSA retains all communications that contain selectors associated with its targets, as well as those that happened to be bundled with them in transit. As discussed further below, NSA analysts may read, query, data-mine, and analyze these communications with few restrictions, and they may share the results of those efforts with the FBI, including in aid of criminal investigations.

50. One aspect of the processes outlined above bears emphasis: Upstream surveillance is not limited to communications sent or received by the NSA's targets. Rather, it involves the surveillance of essentially *everyone's* communications. The NSA systematically examines the full content of substantially all international text-based communications (and many domestic ones) for references to its search terms. In other words, the NSA copies and reviews the communications of millions of innocent people to determine whether they are discussing or reading anything containing the NSA's search terms. The NSA's practice of reviewing the *content* of communications for selectors is sometimes called "about" surveillance. This is because its purpose is to identify not just communications that are to or from the NSA's targets but also those that are merely "about" its targets. This is the digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase. Most pieces of mail—or email—will contain nothing of interest, but the government must still look through each one to find out. Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets; nor does it later purge those communications.

51. Prior to the summer of 2013, the government had not publicly disclosed the fact that, under the FAA, it routinely reviews communications that are neither to nor from its targets. As the Privacy and Civil Liberties Oversight Board observed, "The fact that the

government engages in such collection is not readily apparent from the face of the statute, nor was collection of information 'about' a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act."

Targeting and Minimization Procedures

52. As indicated above, the FAA requires the government to adopt targeting and minimization procedures that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted. These procedures are extremely permissive, and to the extent they impose limitations, those restrictions are riddled with exceptions.

53. Nothing in the targeting procedures meaningfully constrains the government's selection of foreign targets. Nor do the targeting procedures require the government to take measures to avoid intercepting U.S. persons' international communications. The targeting procedures expressly contemplate "about" surveillance, and thus the interception and review of communications between non-targets.

54. The minimization procedures are equally feeble. They impose no affirmative obligation on the NSA to promptly identify and purge U.S. persons' communications once they have been obtained. Rather, they allow the NSA to retain communications gathered via Upstream surveillance for as long as three years by default. It can retain those communications indefinitely if the communications are encrypted; if they are found to contain foreign intelligence information (again, defined broadly); or if they appear to be evidence of a crime. Indeed, the NSA may even retain and share wholly domestic communications obtained through the accidental targeting of U.S. persons if the NSA determines that the communications contain "significant foreign intelligence information" or evidence of a crime. The minimization

procedures also expressly contemplate that the NSA will intercept, retain, and disseminate attorney-client privileged communications. The minimization procedures bar the NSA from querying Upstream data using identifiers associated with specific U.S. persons, but they do not otherwise prohibit the NSA from conducting queries designed to reveal information to, from, or about U.S. persons.

The Surveillance of Plaintiffs

55. Plaintiffs are educational, legal, human rights, and media organizations. Their work requires them to engage in sensitive and sometimes privileged communications, both international and domestic, with journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses, among others.

56. By intercepting, copying, and reviewing substantially all international text-based communications—and many domestic communications as well—as they transit telecommunications networks inside the United States, the government is seizing and searching Plaintiffs' communications in violation of the FAA and the Constitution.

57. The conclusion that the government is seizing and searching Plaintiffs' communications is well-founded for at least four reasons.

58. First, the sheer volume of Plaintiffs' communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of their communications. In the course of a year, Plaintiffs collectively engage in more than one trillion international internet communications. As explained further below, Upstream surveillance could achieve the government's stated goals only if it entailed the copying and review of a large percentage of international text-based traffic. However, even if one assumes a 0.00000001% chance—one one-hundred millionth of one percent—of the NSA copying and reviewing any particular

communication, the odds of the government copying and reviewing at least one of the Plaintiffs' communications in a one-year period would be greater than 99.9999999999%.

59. In reality, this calculation understates the likelihood that the NSA has intercepted, copied, and reviewed Plaintiffs' communications, because large swaths of internet traffic that are not amenable to the text-based searches conducted in the course of Upstream surveillance and are likely of no foreign-intelligence interest to the government. By some estimates, for example, two-thirds of internet traffic consists of video traffic. The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (e.g., Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering, allowing it to more comprehensively monitor text-searchable traffic like that of Plaintiffs.

60. Second, the geographic distribution of Plaintiffs' contacts and communications across the globe makes it virtually certain that the NSA has intercepted, copied, and reviewed Plaintiffs' communications. As noted above, the internet backbone includes the approximately 49 international submarine cables carrying the vast majority of internet traffic into and out of the United States. It also includes the limited number of high-capacity terrestrial cables that carry traffic between major metropolitan areas within the United States, or between the United States and Canada or Mexico. The junctions where these backbone cables meet are in essence "chokepoints"—because almost all international internet traffic (as well as a significant share of domestic traffic) flows through one or more of them. Prime examples are the points where international submarine cables come ashore. The government has acknowledged using

Upstream surveillance to monitor communications at "international Internet link[s]" on the internet backbone.

61. Given the relatively small number of international chokepoints, the immense volume of Plaintiffs' communications, and the fact that Plaintiffs communicate with individuals in virtually every country on earth, Plaintiffs' communications almost certainly traverse every international backbone link connecting the United States with the rest of the world.

62. Third, and relatedly, in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link. That is because, as a technical matter, the government cannot know beforehand which communications will contain selectors associated with its targets, and therefore it must copy and review all international text-based communications transiting that circuit in order to identify those of interest. As the Privacy and Civil Liberties Oversight Board explained with respect to Upstream surveillance, "Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them." Because backbone cables carry vast amounts of internet traffic, the number of communications whose contents will be copied and reviewed will be enormous, regardless of how many the government ultimately retains.

63. There is an even more basic reason that, in conducting Upstream surveillance, the government must be monitoring all the international text-based communications that travel across a given link. To search the contents of any text-based communication for instances of the NSA's "selectors" as that communication traverses a particular backbone link, the

government must first copy and reassemble all of the packets that make up that communication. Those packets travel independently of one another, intermingled with packets of other communications in the stream of data. Where the government seeks to identify communications to, from, or about its many targets, as it does using Upstream surveillance, the packets of interest cannot be segregated from other, unrelated packets in advance. Rather, in order to reliably intercept the communications it seeks, the government must first copy *all* such packets traversing a given backbone link, so that it can reassemble and review the transiting communications in the way it has described.

64. In short, for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals. Accordingly, even if the NSA conducts Upstream surveillance on only a single internet backbone link, it must be intercepting, copying, and reviewing at least those communications of Plaintiffs traversing that link. In fact, however, the NSA has confirmed that it conducts Upstream surveillance at more than one point along the internet backbone, through the compelled assistance of multiple major telecommunications companies.

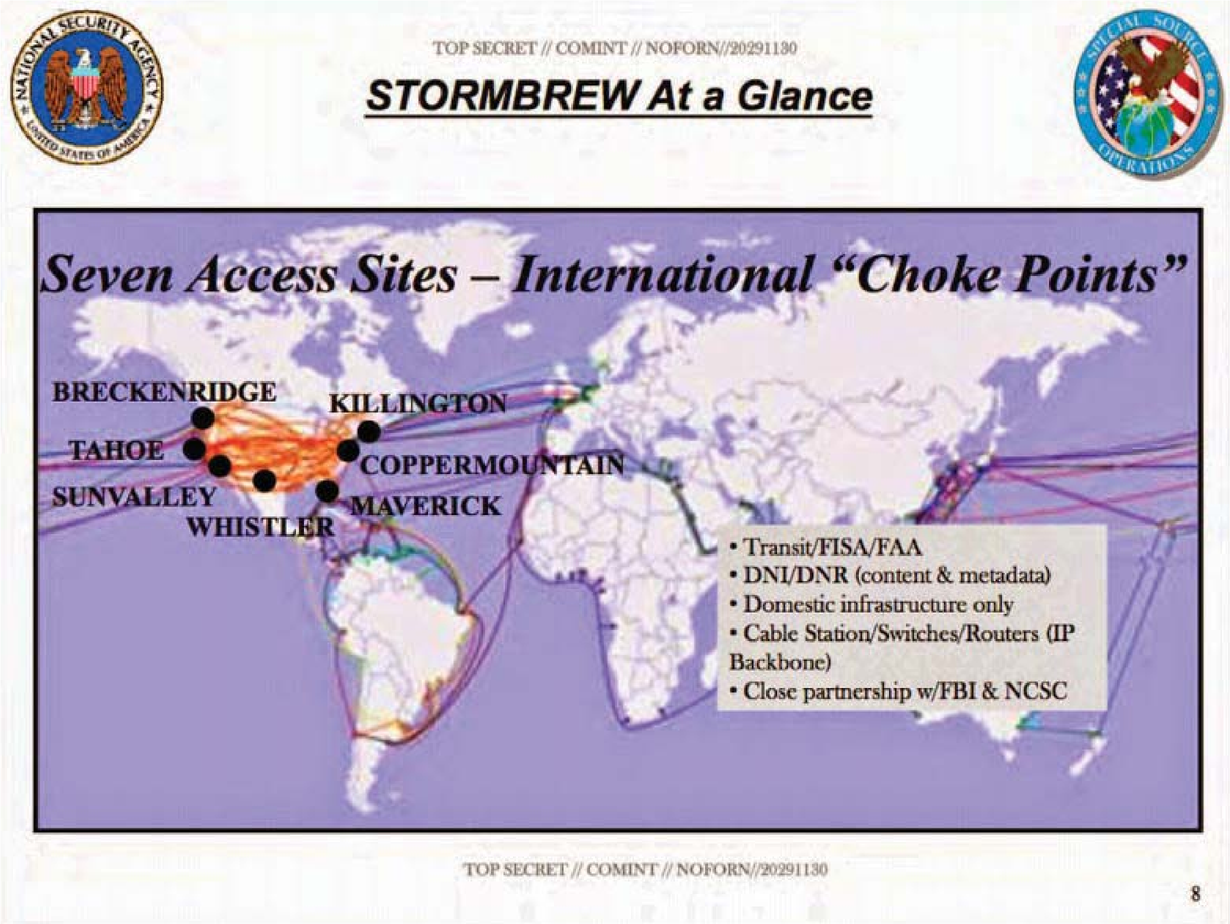
65. Fourth, given the way the government has described Upstream surveillance, it has a strong incentive to intercept communications at as many backbone chokepoints as possible. The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." And it has said about Upstream

surveillance more generally that its "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications."

66. If the government's aim is to "comprehensively" and "reliably" obtain communications to, from, and about targets scattered around the world, it must conduct Upstream surveillance at many different backbone chokepoints. That is especially true because the communications of individual targets may take multiple paths when entering or leaving the United States. When two people communicate in real-time, the communications they exchange frequently take different routes across the internet backbone, even though the end-points are the same. In other words, in the course of a single exchange, the communications *from* a target frequently follow a different path than those *to* the target. Relatedly, a target's location may vary over time, as do the network conditions that determine a given communication's path from origin to destination. As a result, a target's communications may traverse one backbone cable or chokepoint at one moment, but a different one later. In fact, as the Privacy and Civil Liberties Oversight Board observed, even a single email "can be broken up into a number of data packets that take different routes to their common destination." Because of these variables, Upstream surveillance would be comprehensive only if it were implemented at a number of backbone chokepoints.

67. For the four reasons stated above, it is a virtual certainty that the NSA is intercepting, copying, and reviewing Plaintiffs' communications.

68. This conclusion is corroborated by government documents that have been published in the press. For example, one NSA slide illustrates the Upstream surveillance facilitated by just a single provider (referred to as "STORMBREW") at seven major international chokepoints in the United States:


TOP SECRET // COMINT // NOFORN//20291130
STORMBREW At a Glance
Seven Access Sites – International "Choke Points"
BRECKENRIDGE
KILLINGTON
TAHOE
COPPERMOUNTAIN
SUNVALLEY
MAVERICK
WHISTLER
• Transit/FISA/FAA
• DNI/DNR (content & metadata)
• Domestic infrastructure only
• Cable Station/Switches/Routers (IP Backbone)
• Close partnership w/FBI & NCSC
TOP SECRET // COMINT // NOFORN//20291130
8

69. Similarly, another NSA document states that, in support of FAA surveillance, the "NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." In fact, in describing the scale and operation of Upstream surveillance, *The New York Times* has reported, based on interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border."

70. The government's interception, copying, and review of Plaintiffs' communications while in transit is a violation of Plaintiffs' reasonable expectation of privacy in

those communications. It is also a violation of Plaintiffs' right to control those communications and the information they reveal and contain.

71. Furthermore, because of the nature of their communications, and the location and identities of the individuals and groups with whom and about whom they communicate, there is a substantial likelihood that Plaintiffs' communications intercepted by the NSA through Upstream surveillance are retained, read, and disseminated.

72. The retention, reading, and dissemination of Plaintiffs' communications is a further, discrete violation of Plaintiffs' reasonable expectation of privacy in those communications. It is also a further, discrete violation of Plaintiffs' right to control those communications and the information they reveal and contain.

73. Plaintiffs, in connection with constitutionally protected activities, communicate with people whom the government is likely to target when conducting Upstream surveillance, including foreign government officials, journalists, experts, human rights defenders, victims of human rights abuses, and individuals believed to have information relevant to counterterrorism efforts.

74. A significant amount of the information that Plaintiffs exchange over the internet is "foreign intelligence information" within the meaning of the FAA.

75. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs have had to take burdensome and sometimes costly measures to minimize the chance that the confidentiality of their sensitive information will be compromised. Plaintiffs have variously had to develop new protocols for transmitting sensitive information, to travel long distances to collect information that could otherwise have been shared electronically, and in some circumstances to forgo particularly sensitive communications altogether.

76. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs are not able to gather and relay information, represent their clients, and engage in domestic and international advocacy as they would in the absence of the surveillance. Upstream surveillance reduces the likelihood that clients, users, journalists, witnesses, experts, civil society organizations, foreign government officials, victims of human rights abuses, and other individuals will share sensitive information with Plaintiffs.

77. Upstream surveillance is inhibiting the constitutionally protected communications and activities of Plaintiffs and others not before the Court.

Wikimedia Foundation

78. Wikimedia is a non-profit organization dedicated to encouraging the growth, development, and distribution of free, multilingual, educational content. In this effort, it develops and maintains "wiki"-based projects, and provides the full contents of those projects to individuals around the world free of charge. At present, Wikimedia operates twelve free-knowledge projects ("Projects") as well as other related websites and pages on the internet.

79. The best-known of Wikimedia's Projects is Wikipedia—a free internet encyclopedia that is one of the top ten most-visited websites in the world and one of the largest collections of shared knowledge in human history. In 2014, Wikipedia contained more than 33 million articles in over 275 languages, and Wikimedia sites received between approximately 412 and 495 million monthly visitors. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone. Volunteers also use Wikipedia discussion forums and "discussion pages" to debate the editorial policies and decisions required for reliable and neutral content.

80. Other Projects include Wikimedia Commons, an online repository of free images, sound, and other media files; Wikinews, a collaborative journalism platform for volunteers to create and edit original news articles; and Wikibooks, a platform for the creation of free textbooks and annotated texts that anyone can edit consistent with the policies of the site.

81. Wikimedia encourages individuals around the world to contribute to the Projects by communicating information to Wikimedia. Wikimedia receives and maintains this information, and subsequently communicates it to the many other individuals who seek to access, engage with, and further add to Wikimedia's store of knowledge. The principal way in which Wikimedia communicates with its community—which, at its broadest level, consists of individuals who access or contribute to the body of knowledge comprising the twelve Projects—is via the internet.

82. Wikimedia provides the technical infrastructure for the Projects, much of which is hosted on Wikimedia's servers in Virginia, Texas, and California. In addition, Wikimedia develops software and provides tools for others to develop software platforms; develops mobile phone applications and enters into partnerships; administers grants to support activity that benefits the Wikimedia user community and the Wikimedia movement; provides administrative support to grantees; works with community members to organize conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community.

83. Wikimedia maintains an active and close relationship with the volunteers, contributors, and many other users who comprise the Wikimedia community. Wikimedia exists for this community and depends upon it: the user community plays a vital role in many of

Wikimedia's functions, including the creation of Wikimedia content, the development and enforcement of Wikimedia policies, the donation of funds that help Wikimedia thrive, and the governance of the organization as a whole. In short, Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values.

84. Wikimedia's corporate structure and decision-making reflect this interdependence. In accordance with Wikimedia's bylaws, at least half of Wikimedia's Board of Trustees is selected by Wikimedia community members. That Board relies, in turn, on several user-staffed committees to oversee Board elections, consider grant applications, and recommend new Wikimedia chapters or community organizations. More generally, Wikimedia makes core organizational decisions after soliciting the input and preferences of its users on topics including its public-policy positions, the creation of new features and Projects, corporate strategy, and budgetary matters. For instance, Wikimedia staff frequently engage in "Community Consultations," in which community members can offer their views on these and other matters directly.

85. Wikimedia's community of volunteers, contributors, and readers consists of individuals in virtually every country on earth. Among many others, the Wikimedia community includes U.S. persons who are located abroad and who engage in international communications with Wikimedia.

86. Upstream surveillance implicates at least three categories of Wikimedia communications: (i) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other; (ii) Wikimedia's internal "log" communications, which help it to

monitor, study, and improve its community members' use of the Projects; and (iii) communications by Wikimedia staff.

87. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of internet communications. From April 1, 2014 to March 31, 2015, Wikimedia websites received over 255 billion "page views." Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages more than two billion times. Each of these activities involves internet communications between Wikimedia and its users—the majority of whom are located abroad.

88. Indeed, Wikimedia engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth. For a user to view, search, log in, edit, or contribute to a Wikimedia Project webpage, the user's device must send at least one HTTP or HTTPS "request" to a Wikimedia server. "HTTP" and "HTTPS" are common protocols for transmitting data via the internet, including the content of many webpages. The number of requests required for a user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. After receiving such a user request, the Wikimedia server transmits an HTTP or HTTPS "response" to the user's device, where the content of the requested webpage component is rendered and displayed to the user. In May 2015, Wikimedia's U.S.-based servers received more than 88 billion HTTP or HTTPS requests from outside the United States. At this rate, Wikimedia receives more than one trillion HTTP or HTTPS requests annually, and transmits more than one trillion HTTP or HTTPS responses back to those Wikimedia users abroad.

89. Wikimedia's HTTP and HTTPS communications are essential to its organizational mission, as is its ability to control and maintain the privacy of these communications. The communications reveal and contain some of the most sensitive information that Wikimedia possesses: which specific webpages each particular person is editing or visiting. In other words, they reveal who is reading—or writing—what.

90. For example, among other private information, HTTP and HTTPS requests reveal or contain the user's IP address; the URL of the webpage sought by the user, which often conveys information about the content of the requested page; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Many requests also contain other types of private information, such as a user's log-in credentials; the referrer, which reflects information about the previous webpage the user visited; the search terms a user entered to query Wikimedia's webpages; "cookies," which include information that can be used to link a user to his or her prior Wikimedia requests and prior approximate geolocation; a user's non-public "draft" contributions to Wikimedia; or a user's private questions, comments, or complaints, submitted via Wikimedia's online feedback platform.

91. In much the same way, Wikimedia's HTTP and HTTPS responses may reveal or contain, among other private information, the user's IP address; the content of the requested webpage component; the URL of the webpage the user should be redirected to; "cookies," which include information used to link a user to subsequent Wikimedia requests and his or her approximate geolocation; search terms; a user's username; a user's non-public "draft" contributions; and a user's private questions, comments, or complaints.

92. In furtherance of its mission, Wikimedia also frequently engages in communications that permit its users to interact with one another more directly. For example, a

registered user of Wikimedia may send an email via Wikimedia to another registered user, so long as both have enabled email communications on their Wikimedia accounts. Similarly, Wikimedia engages in communications that allow users to interact in small or limited groups—including over wikis that only certain users, such as user-community leaders, have access to, and mailing lists with restricted membership. Some of these communications are transmitted via HTTP or HTTPS; others rely on different protocols. All of these interactions involve communications between Wikimedia and its community members.

93. The second category of Wikimedia communications are its internal, proprietary "log" communications, which help it to monitor, study, and improve the Projects. In particular, every time Wikimedia receives an HTTP or HTTPS request from a person accessing a Project webpage, it creates a corresponding log entry. Among other private information, logs contain the user's IP address; the URL of the webpage sought by the user; the time the request was received by Wikimedia's server; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Depending on the location of the user and the routing of her request, the log may be generated by Wikimedia's servers abroad, which in turn send the log to Wikimedia in the United States. In May 2015, Wikimedia transmitted more than 140 billion logs from its servers abroad to its servers in the United States. The organization relies on its logs for a variety of analytical projects, which are designed to improve Wikimedia's operations and the experience of those using the Projects.

94. Wikimedia's communications with its community members—as well as its internal logs—link each user's page views, searches, and contributions with his or her IP address, as well as with other user-specific information. As a rule, Wikimedia maintains as private the IP addresses associated with its community members and their individual

interactions with the Projects, except in those instances where an individual editor reveals his or her IP address publicly (i.e., is not logged in as a registered user). IP addresses, like telephone numbers, are often personally identifying, especially in conjunction with other information about a given communication or internet user. It is generally trivial to link a particular IP address with a particular person—thereby revealing his or her online activities—in part because internet service providers routinely maintain records of the IP addresses assigned to their network subscribers over time.

95. Because of the information they contain, Wikimedia's communications with its community members, as well as its internal communications related to the study and improvement of the Projects, are often sensitive and private. These communications reveal a detailed picture of the everyday concerns and reading habits of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests.

96. Seizing and searching Wikimedia's communications is akin to seizing and searching the patron records of the largest library in the world—except that Wikimedia's communications provide a more comprehensive and detailed picture of its users' interests than any previous set of library records ever could have offered.

97. Upstream surveillance permits the government to observe—continuously—which of Wikimedia's millions of webpages are being read or edited at any given moment, and by whom. Moreover, it allows the government to review those communications for any reference to its tens of thousands of search terms, and to retain a copy of any communication that is of interest.

98. As an organization, Wikimedia has an acute privacy interest in its communications—one on par with that of users themselves. That is because Wikimedia's

mission and existence depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. Wikimedia's communications reveal who has contributed to the Projects or visited them in search of information—and, just as importantly, exactly *what* information Wikimedia has exchanged with any individual user. With the partial exception of editors who publicly disclose their IP addresses, these exchanges are not public; they are private interactions between Wikimedia and its community members. If it were otherwise, Wikimedia would have immense difficulty both gathering content and sharing information as widely as possible. This privacy is necessary to foster trust with community members and to encourage the growth, development, and distribution of free educational content.

99. Wikimedia's communications also reveal private information about its operations, including details about its technical infrastructure, its data flows, and its member community writ large.

100. Wikimedia takes steps to protect the privacy of its communications and the confidentiality of the information it thereby receives. For instance, because of the sensitivity of Wikimedia's communications with its community members, Wikimedia seeks to collect and retain as little information about those exchanges as possible. Where it does collect such information, Wikimedia strives to keep it for only a limited amount of time, consistent with the maintenance, understanding, and improvement of the Projects and with Wikimedia's legal obligations. Still, Wikimedia possesses a large volume of sensitive information about its interactions with its community members, and it transmits a large volume of sensitive information about those interactions every day.

101. Wikimedia defends the privacy of its communications in other ways, including through both technical measures and legal action. Wikimedia undertakes costly and burdensome measures to ensure the security of its communications and the data it retains as a result. Wikimedia also assures its community via policies, public statements, and guidelines that it will reject third-party requests for non-public user information unless it is legally required to disclose that information. In keeping with these assurances, Wikimedia resists third-party demands for information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Projects.

102. Wikimedia also engages in a third category of sensitive communications. Certain members of Wikimedia's staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out Wikimedia's work.

103. Wikimedia's communications—with its community members, its internal communications, and its staff communications—are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Wikimedia, its staff, and its users, and it violates their right to control those communications and the information they contain.

104. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Wikimedia's international communications because Wikimedia is communicating with or about persons the government has targeted for Upstream surveillance. Wikimedia's international contacts include foreign telecommunications companies, foreign government

officials, political and business leaders, universities, Wikimedia users and their legal counsel, Wikimedia trustees and international contractors, Wikimedia's international outside legal counsel, project partners, grantees, and volunteers—some of whom are likely targets. Wikimedia's communications with these contacts sometimes concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Wikimedia communicates both with and about these likely targets. Wikimedia's international communications contain, among other things, information about its foreign contacts, including the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Wikimedia's work.

105. Moreover, more than one trillion of Wikimedia's international communications each year—its HTTP and HTTPS transmissions as well as its internal logs of user activity—contain details such as website addresses and IP addresses. Whenever a Wikimedia user abroad edits or contributes to a Project webpage that happens to reference one of the NSA's selectors, Wikimedia engages in an international communication containing that selector. The same is often true when a Wikimedia user abroad simply reads such a Project webpage. Some of these communications are likely retained, read, and disseminated in the course of Upstream surveillance.

106. Because Wikipedia is a comprehensive encyclopedic resource, it includes entries related to virtually any foreign organization or company the U.S. government might target for Upstream surveillance. Many of these entries contain website addresses and domain names associated with those likely targets. Notably, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization list appear over 700 times on Project webpages—including those describing organizations, like

Uzbekistan's Islamic Jihad Union, whose communications the U.S. government has targeted using FAA surveillance.

107. The NSA has expressed interest in surveilling Wikimedia's communications. An NSA slide disclosed by the media asks, "Why are we interested in HTTP?" It then answers its own question: "Because nearly everything a typical user does on the Internet uses HTTP." This statement is surrounded by the logos of major internet companies and websites, including Facebook, Yahoo, Twitter, CNN.com, and Wikipedia. The slide indicates that, by monitoring HTTP communications, the NSA can observe "nearly everything a typical user does" online—including individuals' online reading habits and other internet activities. This information is queried and reviewed by analysts using a search tool that allows NSA analysts to examine data intercepted pursuant to the FAA and other authorities.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Why are we interested in HTTP?
facebook
YAHOO!
twitter
myspace.com
a place for friends
Because nearly everything a typical user does on the Internet uses HTTP
CNN.com
Google
Earth
Gmail
@mail.ru
WIKIPEDIA
The Free Encyclopedia

108. Upstream surveillance undermines Wikimedia's ability to conduct its work. Wikimedia depends on its ability to ensure anonymity for individuals abroad who view, edit, or otherwise use Wikimedia Projects and related webpages. The ability to read, research, and write anonymously is essential to the freedoms of expression and inquiry. In addition, Wikimedia's staff depend on the confidentiality of their communications, including in some cases their ability to ensure that their contacts' identities will not be revealed. Because of these twin needs for anonymity and confidentiality, Upstream surveillance harms the ability of Wikimedia's staff to engage in communications essential to their work and compromises Wikimedia's organizational mission by making online access to knowledge a vehicle for U.S. government monitoring.

109. Due in part to NSA surveillance, including Upstream surveillance, Wikimedia has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances self-censoring communications or forgoing electronic communications altogether. These measures divert Wikimedia's time and monetary resources as a non-profit entity from other important organizational work.

110. Despite these precautions, Wikimedia believes that Upstream surveillance has resulted and will result in some foreign readers, editors, contributors, and volunteers being less willing to read, contribute to, or otherwise engage with Wikimedia's Projects. For instance, some Wikimedia users have expressed reluctance to continue participating in the Wikimedia movement because of U.S. government surveillance, including FAA surveillance. The loss of these foreign users is a direct detriment to Wikimedia, its ability to receive information and associate with its community members, and its organizational goal of increasing global access

to knowledge. It also harms Wikimedia's domestic users, who do not have access to information and opinions that Wikipedia's foreign contributors would otherwise have provided. Similarly, Wikimedia believes that Upstream surveillance reduces the likelihood that Wikimedia's foreign volunteers, grantees, and other contacts will communicate with staff members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

111. Because Wikimedia's community members are so numerous, because they are dispersed across the globe, and because millions of them choose to interact with Wikimedia anonymously, their rights are likely to be impaired if Wikimedia is unable to assert claims on their behalf. That is especially so because Wikimedia is uniquely capable of presenting the aggregate effects that Upstream surveillance has on community members' ability to contribute to the Projects and to receive information from others.

National Association of Criminal Defense Lawyers

112. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL's mission is to foster the integrity, independence, and expertise of the criminal defense profession, and to promote the proper and fair administration of justice. NACDL has approximately 9,200 members as well as 90 local, state, and international affiliate organizations with approximately 40,000 members. NACDL's interest in challenging the lawfulness of Upstream surveillance is germane to the organization's mission and purpose, and to its relationship with its members. As explained below, because unlawful U.S. government surveillance profoundly affects the ability of

criminal defense attorneys to ensure that accused persons receive effective counsel, such surveillance interferes with the proper and fair administration of justice.

113. As defense attorneys, NACDL's members engage in international and domestic internet communications that are essential to the effective representation of their clients. Among other things, NACDL's members routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad as part of their representations.

114. The communications of NACDL's members are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of members' communications and it violates their right to control their communications and the information they contain.

115. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates international communications of NACDL's members because they are communicating with or about persons the government has targeted for Upstream surveillance. In the course of their representations, NACDL members communicate internationally with clients, clients' families, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Their communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." NACDL members communicate both with and about these likely targets. Members' international communications contain, among other things, details about their foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to their work.

116. One group of NACDL members is especially likely to have their communications retained, read, and disseminated in the course of Upstream surveillance: defense attorneys who represent individuals in criminal prosecutions in which the government has acknowledged its use FAA surveillance. In these cases, the government's prosecution of the defendant is based on evidence obtained from an FAA target. As a result, defense attorneys are especially likely to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting their own evidence. Indeed, in several of these cases, the targeted selector—*e.g.*, the targeted email address—has been identified in press reports or may be ascertained from congressional testimony and court filings. NACDL defense attorneys who communicate internationally with or about that targeted selector will have their communications retained by the government, much as their clients' communications were warrantlessly intercepted and retained.

117. NACDL members have an ethical obligation to protect the confidentiality of their clients' information, including information covered by the attorney-client privilege.

118. Upstream surveillance compromises NACDL members' ability to comply with their ethical obligations and undermines their effective representation of their clients. Members' defense work depends on the confidentiality of their communications, including their ability to assure contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, NACDL's members have undertaken burdensome and costly measures to protect their communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, NACDL believes that

Upstream surveillance reduces the likelihood that potential sources, witnesses, experts, and foreign government officials will share sensitive information with NACDL's members, because those contacts fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

NACDL Member Joshua L. Dratel

119. Joshua L. Dratel is a nationally recognized criminal defense lawyer in New York City who has been a member of NACDL since 1985. He is Chair of NACDL's National Security Committee, co-Chair of NACDL's Select Committee on Military Tribunals, and Co-Chair of its Amicus Curiae Committee. From 2003 to 2009, he served as a member of the Board of Directors of NACDL. He is also co-editor of *The Torture Papers: The Legal Road to Abu Ghraib* (Cambridge University Press 2005).

120. Mr. Dratel's litigation experience encompasses all aspects of criminal defense, and among other clients, he represents individuals accused of internet- and terrorism-related crimes. For example, he defended Wadith El Hage in *United States v. Usama Bin Laden*, the prosecution resulting from the 1998 bombings of the U.S. embassies in Kenya and Tanzania. Mr. Dratel also represented David Hicks—who was detained at Guantánamo Bay for six years—in U.S. military commission proceedings. The U.S. Court of Military Commission Review recently overturned Mr. Hicks's conviction for material support for terrorism. Mr. Dratel's current clients include Baasaly Moalin, who is appealing from a conviction of charges of material support for terrorism.

121. Mr. Dratel's law practice also includes a client who has received notice of FAA surveillance, and he previously represented a client in another case where officials have told

Congress that the government used FAA surveillance in the course of its investigation. He has defended other individuals in prosecutions where there is reason to believe the government relied on such surveillance.

122. In connection with his defense work and confidential consultations with defense attorneys in other national security-related cases, Mr. Dratel routinely engages in both domestic and international communications via the internet. Many of the individuals with whom he exchanges information are located abroad, and are neither U.S. citizens nor permanent residents. Their communications occur via email, instant messenger, and text messaging.

123. The vast majority of Mr. Dratel's international communications as a defense attorney are sensitive, and many of them are privileged or otherwise protected from disclosure by the attorney work-product doctrine.

124. Mr. Dratel's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of his communications and it violates his right to control his communications and the information they contain.

125. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating with persons the government has targeted for Upstream surveillance. In the course of his representations, Mr. Dratel communicates internationally with clients, clients' families, lawyers, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Most notably, his international contacts include individuals the U.S. government has targeted for prosecution for terrorism-related crimes, as well as their families, friends, and associates, including their attorneys overseas. For example, Mr. Dratel communicates via the internet with his former client, Mr. Hicks, who lives

in Australia following his release from Guantánamo Bay. In addition, Mr. Dratel's communications with his international contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Mr. Dratel also communicates with likely FAA targets when he visits websites hosted overseas on the internet. This internet browsing involves communications with selectors—such as domain names and IP addresses—that the NSA has likely targeted for FAA surveillance. In his representation of defendants charged with terrorism-related crimes, it is often necessary for him to review websites maintained by terrorist organizations abroad, so that he can understand the facts related to certain investigations and prosecutions.

126. Similarly, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating *about* persons the government has targeted for Upstream surveillance. Mr. Dratel's international communications contain, among other things, details about his foreign contacts and other important sources of information—details such as the email addresses, phone numbers, social media identities, and website addresses of foreign individuals and organizations relevant to his work.

127. The fact that Mr. Dratel's clients have been subject to FAA surveillance themselves, or involved in investigations where others were subject to such surveillance, makes the NSA's retention and dissemination of Mr. Dratel's own communications especially likely. In representing these clients, Mr. Dratel is almost certain to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting evidence abroad via the internet. When Mr. Dratel

communicates with or about persons and selectors targeted under the FAA, he is subject to FAA surveillance just like his clients.

128. Due in part to U.S. government surveillance, including Upstream surveillance, Mr. Dratel has had to undertake burdensome and costly measures to protect his international communications, and in certain instances has forgone those communications altogether. For example, Mr. Dratel has had to and will have to travel abroad to gather information in-person that he would otherwise have gathered by electronic communication. Such travel is time-consuming and costly. He has also paid for and will have to pay for investigators abroad to travel to the United States to meet with him in-person to discuss their cases. In addition, Mr. Dratel routinely relies on time-consuming security measures, such as Pidgin Encryption and PGP, to encrypt his domestic and international instant messages and emails, in an effort to protect especially sensitive privileged communications and work product. Mr. Dratel also routinely censors his own speech (and asks his international contacts to do the same) in electronic communications. These precautions and security measures are not voluntary; they are the result of Upstream surveillance and the rules of professional responsibility that apply to Mr. Dratel as an attorney.

129. As a general matter, Upstream surveillance compromises Mr. Dratel's ability to communicate with his clients overseas and to gather information relevant and necessary to his work. This surveillance makes it difficult, expensive, and sometimes impossible to obtain information from individuals outside of the United States. In some instances, the increased awareness of U.S. government surveillance has resulted and will result in clients, lawyers, and potential witnesses limiting the information that they share with Mr. Dratel and that he shares with them. Indeed, some witnesses abroad have not and will not communicate with Mr. Dratel

at all electronically, because they believe that by sharing information with him, they are also sharing information with the U.S. government. At times, Mr. Dratel must forgo these communications altogether. The cost of traveling to certain remote areas of the globe to interview a potential witness in-person can be too high to justify the travel, and some regions are simply too dangerous or inaccessible to permit in-person visits.

Human Rights Watch

130. HRW is a non-profit, non-governmental human rights organization based in New York City. It employs approximately 400 staff members located across offices around the world. Formed in 1978, HRW's mission is to defend the rights of people worldwide. HRW conducts fact-finding investigations into human rights abuses by governments and non-state actors in all regions of the world.

131. HRW engages in international and domestic internet communications that are essential to its mission. Among other things, HRW's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out HRW's research, reporting, and advocacy work.

132. HRW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of HRW's communications and it violates HRW's right to control those communications and the information they contain.

133. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates HRW's international communications because HRW is communicating with or about persons the government has targeted for Upstream surveillance. HRW's international contacts include foreign government officials, humanitarian agencies, think tanks, military officials, human rights defenders, politicians, dissidents, victims of human rights abuses,

perpetrators of human rights abuses, religious groups, media, and scholars, some of whom are likely targets. HRW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." HRW communicates both with and about these likely targets. HRW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to HRW's work.

134. Upstream surveillance undermines HRW's ability to conduct its work. HRW's research, reporting, and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, HRW has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, HRW believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with HRW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Amnesty International USA

135. AIUSA, headquartered in New York City, is one of Amnesty International's largest national sections, with hundreds of thousands of members and supporters. Through its

advocacy campaigns, AIUSA seeks to expose and stop human rights abuses in the United States and throughout the world.

136. AIUSA engages in international and domestic internet communications that are essential to its mission. Among other things, some of AIUSA's U.S.-based staff—as well as some AIUSA members who serve as volunteer specialists on particular countries and thematic issues—routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out AIUSA's reporting and advocacy work.

137. AIUSA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of AIUSA's communications and it violates AIUSA's right to control those communications and the information they contain.

138. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates AIUSA's international communications because AIUSA is communicating with or about persons the government has targeted for Upstream surveillance. AIUSA's international contacts include Amnesty International researchers who are documenting and witnessing human rights violations in the field, human rights defenders, victims of violations and their families, eyewitnesses to violations, political dissidents, government officials, journalists, and lawyers, some of whom are likely targets. AIUSA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." AIUSA communicates both with and about these likely targets. AIUSA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to AIUSA's work.

139. Upstream surveillance undermines AIUSA's ability to conduct its work. AIUSA's reporting and advocacy depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, some AIUSA staff strive to communicate particularly sensitive matters in-person, and must sometimes avoid sensitive topics or forgo exchanging information about these matters altogether. Despite these precautions, AIUSA believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with AIUSA's staff and members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

PEN American Center

140. PEN is an association based in New York City of approximately 4,000 novelists, journalists, editors, poets, essayists, playwrights, publishers, translators, agents, and other professionals, and an even larger network of readers and supporters. It is the largest of the organizations within PEN International. For the last 90 years, PEN has worked to ensure that people all over the world are at liberty to create literature, to convey ideas freely, and to express their views unimpeded. One of PEN's core projects is to advocate on behalf of persecuted writers across the globe, so that they might be free to write and to express their ideas.

141. PEN engages in international and domestic internet communications that are essential to its mission. Among other things, PEN's U.S.-based staff routinely engage in

sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out PEN's research and advocacy work.

142. PEN's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of PEN's communications and it violates PEN's right to control those communications and the information they contain.

143. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates PEN's international communications because PEN is communicating with or about persons the government has targeted for Upstream surveillance. PEN's international contacts include writers whose work and experiences relate to political upheavals, human rights violations, freedom of the press, and government surveillance; those writers' families and legal representatives; human rights defenders; and other PEN partners in countries such as Syria, Cuba, China, Iran, and Ethiopia—some of whom are likely targets. PEN's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." PEN communicates both with and about these likely targets. PEN's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to PEN's work.

144. Upstream surveillance undermines PEN's ability to conduct its work. PEN's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, PEN staff have undertaken burdensome measures to secure and protect their

communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, PEN believes that Upstream surveillance reduces the likelihood that foreign writers and other contacts will share sensitive information with PEN's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Global Fund for Women

145. GFW, based in San Francisco and New York City, is a grant-maker and a global advocate for women's human rights. GFW advances the movement for women's human rights by directing resources to and raising the voices of women worldwide. GFW invests in local, courageous women and women-led organizations, and creates digital advocacy campaigns on critical global issues for women and girls. Since its inception in 1986, GFW has awarded 9,921 grants totaling $120 million to 4,759 organizations in 175 countries.

146. GFW engages in international and domestic internet communications that are essential to its mission. Among other things, GFW's U.S.-based staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out GFW's grant-making and advocacy work.

147. GFW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of GFW's communications and it violates GFW's right to control those communications and the information they contain.

148. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates GFW's international communications because GFW is communicating with or

about persons the government has targeted for Upstream surveillance. GFW's international contacts include foreign banks, foreign government agencies, funders, attorneys, and grantee and partner organizations working in conflict zones or on politically sensitive issues abroad, some of whom are likely targets. GFW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." GFW communicates both with and about these likely targets. GFW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to GFW's work.

149. Upstream surveillance undermines GFW's ability to conduct its work. GFW's grant-making depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, GFW's staff must exercise extreme caution when engaging in certain international communications, and in some instances avoid sensitive topics or forgo communications altogether. Some of GFW's international contacts will communicate with the organization only by phone or Skype, rather than email, because they believe that email is a less secure means of communication. Other of GFW's international contacts will communicate via email, but only if staff avoid using certain words in their communications that may result in further government scrutiny. Despite these precautions, GFW believes that Upstream surveillance reduces the likelihood that current and prospective grantees will share sensitive information with GFW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the

other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Nation Magazine

150. The Nation is America's oldest weekly magazine of opinion, news, and culture. The Nation is also a digital media company, reporting daily on politics, social issues, and the arts. Its journalists report on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities and politics in China and elsewhere in East Asia, and civil wars and other conflicts in Africa and Latin America.

151. The Nation engages in international and domestic internet communications that are essential to its mission. Among other things, The Nation's staff and contributing writers routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out The Nation's research, reporting, and editing.

152. The Nation's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of The Nation's communications and it violates The Nation's right to control those communications and the information they contain.

153. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates The Nation's international communications because The Nation is communicating with or about persons the government has targeted for Upstream surveillance. The Nation's international contacts include foreign journalists in conflict zones, foreign government officials, political dissidents, human rights activists, and members of guerrilla and insurgency movements, some of whom are likely targets. The Nation's communications with these

contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." The Nation communicates both with and about these likely targets. The Nation's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to The Nation's work.

154. Upstream surveillance undermines The Nation's ability to conduct its work. The Nation's research and reporting depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, The Nation has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, The Nation believes that Upstream surveillance reduces the likelihood that foreign journalists and sources will share sensitive information with The Nation, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Rutherford Institute

155. The Rutherford Institute, founded in 1982 and based in Virginia, is a civil liberties organization committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties

and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments.

156. Rutherford engages in international and domestic internet communications that are essential to its mission. Among other things, Rutherford's staff, who are based in the U.S., routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out Rutherford's advocacy, legal, and educational activities.

157. Rutherford's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Rutherford's communications, and it violates Rutherford's right to control those communications and the information they contain.

158. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Rutherford's international communications because Rutherford is communicating with or about persons the government has targeted for Upstream surveillance. Rutherford's international contacts include human rights and civil liberties advocates, foreign government officials, and individuals whose rights are threatened by the U.S. or foreign governments, some of whom are likely targets. Rutherford's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Rutherford communicates both with and about these likely targets. Rutherford's international communications, among other things, contain details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Rutherford's work.

159. Upstream surveillance undermines Rutherford's ability to conduct its work. Rutherford's advocacy depends on its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, Rutherford in some instances avoids sensitive topics or forgoes communications altogether. Rutherford believes that Upstream surveillance reduces the likelihood that victims of human rights abuses, witnesses, foreign government officials, and other contacts will share sensitive information with Rutherford, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Washington Office on Latin America

160. WOLA is a non-profit, non-governmental organization based in Washington D.C. WOLA works to advance human rights and social justice in the Americas. WOLA is regularly called upon for its research and analysis by policymakers, the media, and academics in the U.S. and Latin America. To further this work, WOLA gathers and publishes information about U.S. policies concerning Latin America, U.S. assistance (military or otherwise) to Latin American countries, and U.S. immigration practices, among other things.

161. WOLA engages in international and domestic internet communications that are essential to its mission. Among other things, WOLA's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out WOLA's research, policy, and advocacy work.

162. WOLA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of WOLA's communications and it violates WOLA's right to control those communications and the information they contain.

163. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates WOLA's international communications because WOLA is communicating with or about persons the government has targeted for Upstream surveillance. For instance, WOLA communicates with foreign government officials located abroad—including at times presidents and foreign ministers. Similarly, it communicates with policymakers, academics, journalists, human rights defenders, victims of human rights abuses, and staff from multilateral institutions, such as the Organization of American States, the Inter-American Development Bank, and the United Nations, some of whom are also likely targets. WOLA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." WOLA communicates both with and about these likely targets. WOLA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to WOLA's work.

164. Upstream surveillance undermines WOLA's ability to conduct its work. WOLA's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, WOLA has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication,

traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, WOLA believes that Upstream surveillance reduces the likelihood that policymakers, foreign government officials, experts, witnesses, and victims of human rights abuses will share sensitive information with WOLA's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

CAUSES OF ACTION

165. Upstream surveillance exceeds the authority granted by 50 U.S.C. § 1881a, and therefore violates 5 U.S.C. § 706.

166. Upstream surveillance violates the Fourth Amendment to the Constitution.

167. Upstream surveillance violates the First Amendment to the Constitution.

168. Upstream surveillance violates Article III of the Constitution.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs respectfully request that the Court:

1. Exercise jurisdiction over Plaintiffs' Complaint;

2. Declare that Upstream surveillance violates 50 U.S.C. § 1881a and 5 U.S.C. § 706;

3. Declare that Upstream surveillance is unconstitutional under the First and Fourth Amendments, and under Article III;

4. Permanently enjoin Defendants from continuing Upstream surveillance;

5. Order Defendants to purge all records of Plaintiffs' communications in their possession obtained pursuant to Upstream surveillance;

6. Award Plaintiffs fees and costs pursuant to 28 U.S.C. § 2412;

7. Grant such other and further relief as the Court deems just and proper.

Dated: June 19, 2015
Baltimore, Maryland

Respectfully submitted,

/s/ Deborah A. Jeon
Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

/s/ Patrick Toomey
Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
(*signed by Patrick Toomey with permission of Debbie A. Jeon*)
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)

csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

UNITED STATES DISTRICT COURT

DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS; HUMAN RIGHTS WATCH; AMNESTY INTERNATIONAL USA; PEN AMERICAN CENTER; GLOBAL FUND FOR WOMEN; THE NATION MAGAZINE; THE RUTHERFORD INSTITUTE; and WASHINGTON OFFICE ON LATIN AMERICA, *Plaintiffs*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE; ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE; JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; DEPARTMENT OF JUSTICE; and ERIC H. HOLDER, in his official capacity as Attorney General of the United States, *Defendants*.	Hon. T. S. Ellis III No. 15-cv-00662-TSE

DECLARATION OF DR. ALAN SALZBERG

I, Dr. Alan Salzberg, do hereby state and declare as follows:

Introduction

1. I am the Principal (and owner) of Salt Hill Statistical Consulting. My work includes statistical sampling, analysis, and review for government and industry. On several occasions, I have written expert statistical reports or testified as a statistical expert, both in court and in depositions.
2. I received a Ph.D. in Statistics from the University of Pennsylvania, where I also received a B.S. in Economics. I have taught courses in statistics and quantitative methods at the University of Pennsylvania and American University and have published several statistics papers in peer-reviewed journals. I am also the co-inventor on a U.S. Patent (#6,636,585) for a statistical process design to test the systems of telecommunications companies. A copy of my resume is attached as an appendix to this report.
3. My current and recent work includes: statistical sampling and analysis of financial records on behalf of the United States Geological Survey; statistical review of the sampling and estimation methodology used to audit Medicaid providers in New York State on behalf of the New York State Office of Medicaid Inspector General; analysis of failure rates and survival modeling regarding the chances of catastrophic failure of an undersea oil field on behalf of a major construction company; statistical sampling and analysis, including regression modeling and survival analysis, on behalf of the U.S. Department of Labor; statistical modeling and prediction related to determining the number of prescriptions filled for a variety of pharmaceutical products in separate projects for a pharmaceutical company and for an industry data provider; review and testing of telecommunications data and statistical methods on behalf of public service commissions (including statistical sampling).

4. The purpose of this declaration is to assess the claim and accompanying probability calculation found in paragraph 58 of Wikimedia's First Amended Complaint, which states that "the odds of the government copying and reviewing at least one of the Plaintiffs' communications in a one-year period would be greater than 99.9999999999%." Compl. ¶ 58. This declaration reviews that statistical claim, explaining the necessary assumptions under which it would be correct and incorrect. The declaration first summarizes my findings and then provides details of the analysis that led to these conclusions.

Summary of Findings

5. The Plaintiffs give no statistical foundation in the Complaint for three assumptions[1] necessary to the calculation in paragraph 58 of the Complaint. These assumptions are:

   a. There is a 0.00000001% chance that the NSA copies and reviews any one communication.

   b. The chance of copying and review for each communication is the same; and

   c. The fact that one communication was or was not copied and reviewed does not affect the chances of the copy and review of any other communication.

6. As I explain below, each of these assumptions are unsupported by any statistical foundation in the Complaint. The assumptions are nevertheless necessary to support the

[1] Plaintiffs also assume that their collective number of international communications per year is more than one trillion. This appears to be based, in large part, on "88 billion HTTP or HTTPS requests" to/from Wikimedia websites, cited in paragraph 88, for May 2015. This number is presumably multiplied by 12 months to arrive at one trillion per year, *see* Compl. ¶ 88. The unstated assumptions regarding these requests are that all twelve months over the last year maintained the same number of communications and that any HTTP request is a "communication."

calculations made in the Complaint, and Plaintiffs' calculation would be invalid if any one of these assumptions is not correct.

7. Moreover, even if the calculation were correct that it is highly probable that at least one communication of one of the nine Plaintiffs' were copied and reviewed, it does not indicate that *each* of the nine Plaintiffs' communications were copied and reviewed. In fact, these chances could be far smaller, as I explain below.

8. Based on my analysis below, it is not statistically inconsistent for the NSA to have reviewed a very large number of communications but still have reviewed none of the Plaintiffs' communications.

Detailed Findings

9. Paragraph 58 of the Complaint performs a calculation regarding "the odds of the government copying and reviewing at least one of the Plaintiffs' communications." Compl. ¶ 58. The calculation puts those chances at greater than 99.9999999999%, a number that for all practical purposes is 100%. However, the calculation of these chances requires a number of assumptions.

10. The calculation is based on a statistical probability distribution called the binomial distribution. This distribution requires the assumptions that the number of items (communications) is known, that the chances of copying and reviewing are known and the same for each communication (statistically, this is called "identically distributed"), and that that the copying or reviewing of one communication has no effect on the chances

of copying and reviewing any other communication (statistically, this is called "independence of observations").[2]

11. The first assumption, that the chances of copying and reviewing any one communication is known and is equal to 0.00000001% is set forth specifically in paragraph 58, but no statistical foundation is provided for it in the Complaint. If that assumption is incorrect, the calculation changes as a direct result. For instance, if the chance of copying and reviewing any one communication is equal to 0.00000000001% instead of 0.00000001%, the chances that at least one Plaintiff communication is copied and reviewed falls to 10%, even assuming the total number of Plaintiff communications is equal to more than one trillion. Further, if the chance of copying and reviewing any one communication is equal to 0.000000000001%, the chances that at least one of Plaintiffs' communications is reviewed falls to 1%. In this way, the validity of this assumption can drastically affect the conclusion set forth in paragraph 58 of the Complaint.

12. When Plaintiffs' assumptions are applied in determining the chances that at least one communication for a particular Plaintiff was copied and reviewed, the chances fall, because whatever the totality of Plaintiffs' communications are, each particular Plaintiff will have less than that total. So even if the calculation were correct that it is highly probable that at least one of the nine Plaintiffs' communications were copied and reviewed, the chances that any particular Plaintiff's communications were copied and reviewed depends (at least in part) on the total number of communications for that Plaintiff and is lower than the percentage chance set forth in paragraph 58.

---

[2] For my calculations, I used the R language function pbinom. The same can also be accomplished using the Poisson distribution in a situation in which typical calculators cannot precisely perform the calculation.

13. In order to perform the exact calculation, we would need to know the total number of communications for that particular Plaintiff. For example, if Plaintiff The Rutherford Institute of Charlottesville, Virginia, had one million communications each year, then the chances that at least one of that Plaintiff's communications (as opposed to Plaintiff Wikimedia's communications) would be copied and reviewed would be only about 1 in 10,000 (0.01%); this calculation assumes, of course, that the chance of copying and reviewing any one particular Plaintiff's communication remains the same as stated in paragraph 58 (0.00000001%).

14. The two implicit assumptions of "independence" and "identically distributed" (often grouped together and called "iid") are also critical to the calculation. The iid assumptions mean that the chances of copying and reviewing are the same for all communications and that the chances of any one item being copied and reviewed does not vary based on whether any other item is copied and reviewed. Thus, the assumption means communications from anywhere in the world all have equal chances of being copied and reviewed, such that the chance of copying and reviewing of a communication by someone in Iran is the same as the chance of copying and reviewing a communication by someone in Ireland. Furthermore, these assumptions also mean that if a communication sent from Iran from a particular computer at a certain time was copied and reviewed, the chances that a communication sent from that same computer one second later has no more or less chance of being copied than the original 0.00000001%.

15. Any clustering of the copying and reviewing of communications, whether by country or some other criteria, would mean that some groups would have different chances of being copied than some other groups and that the fact that a particular communication in one

group is reviewed or copied means other communications in that group are more likely to be copied.

16. The iid assumptions are sweeping but are nonetheless necessary for the calculation to be correct. In order to account for or remove them, we would need to know the specific chances that are appropriate to apply to Plaintiffs' communications and the exact nature of how the Plaintiffs' communications are clustered.

17. By way of illustration of the iid assumptions, consider a statistical survey that selects people at random from some population. Such a survey has a selection method that is iid—selection of one person provides no information on whether another person is sampled and the chances of any one person being selected are the same. Only careful attendance to the mechanics of the survey—delineation of all possible respondents and statistically random sampling of a set of them—can ensure that the survey is truly random and that the iid property holds.

18. A statistically haphazard survey will generally be far from random. Consider a survey, even a very large one, where someone stands on a street corner and questions passers-by. This survey is certainly haphazard in design, and it is equally certainly not random. For example, even if it is known that on a random day 10% of people in the U.S. carry umbrellas, a survey done in Phoenix on a sunny summer day is unlikely to yield any people with umbrellas while one done in Seattle on a rainy winter day is likely to yield many. The assumptions the Plaintiffs use would say that if 1,000 are surveyed, then there

is a greater than a 99.9999999999% chance someone surveyed will be carrying an umbrella without regard to whether the survey was in Seattle or Phoenix.[3]

19. Likewise, even a very large operation of copying and reviewing communications may completely miss some communication while copying and reviewing nearly 100% of others. To be accurate, the Plaintiffs' calculation requires that the copying and review of communications be like a good statistical survey in that the selection for copying and reviewing is random. But Plaintiffs' assertions about how the process works—through the copying of "*certain* high-capacity cables, switches, and routers" (Compl. ¶ 49)—would mean, if accurate, that the process is, in statistical terms, haphazard like the survey

[3] These two assumptions are also critical to the accuracy of percentage chances in the scenario of an hourly forecast of rain. Suppose that the chances of rain any morning hour between 9 and noon are 0.6, or 60%. If this is the case and the chances are iid in each of the three hours 9am to 10am, 10am to 11am and 11am to noon, then the chances of *no* rain in any hour is 40% (100% - 60%), or 0.4, to the power of 3, which equals 6.4%. If the identically distributed assumption is violated the chances of rain could average 60% but would be different each hour. Thus, the chances in the first hour could be 100% and the chance in each of the next two hours could be 40%, a combination which still produces an average of 60%. However, the chance of no rain is 0 rather than 6.4% since during the first hour the chance of rain is 100%. And if the independence assumption is violated, the chances may be correct at 60% per hour, but, if it is not raining the first hour, it may be very unlikely it will rain in either of the other two. In this case, the chance of no rain would be 40% for the first hour, but 0% in the second and third hour if it does not rain in the first hour (and 100% in the second and third hour if it does rain the first hour). This would be the case if a storm that lasts three hours may or may not hit the area. If it does hit the area, it will begin between 9am and 10am and continue through noon. In this case, the chances of no rain between nine and noon are 40%. This example also shows that without the iid assumption, which allows the chances for each time period to be treated independently and all chances to be assumed to be the same, the calculation of the chances can be far different than with the assumption.

with the umbrellas.[4] Therefore, the statistical assumptions Plaintiffs have made in paragraph 58 are inconsistent with how they say this copying and reviewing process works. Using my earlier example of the umbrella survey, Plaintiffs have calculated the chances of any one person carrying an umbrella by using a studiously random statistical model to determine how many people are carrying an umbrella without regard for whether the survey itself occurred in Phoenix on a summer day or on a rainy day in Seattle in the winter. In terms of the umbrella survey, however, Plaintiffs have tried to apply that statistically random model to a statistically haphazard survey that occurs in certain cities at a certain time of the year.

20. In conclusion, the chances calculated in paragraph 58 of the Complaint depend on assumptions for which no statistical basis is provided in the Complaint. If any of these assumptions are incorrect—and Plaintiffs' description of the process of copying and review suggest that these assumptions are incorrect—then the chances of one of Plaintiffs' communications being copied and reviewed could be far less than 100%.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: August 4, 2015

Alan Salzberg

Digitally signed by Alan Salzberg
DN: cn=Alan Salzberg, o=Salt Hill Statistical Consulting, ou, email=salzberg@salthillstatistics.com, c=US
Date: 2015.08.04 08:13:28 -04'00'

ALAN SALZBERG

[4] Such a method of copying and reviewing, if the NSA does in fact use that method, may mean that Plaintiffs' communications have no chance of being copied, as would be the case if Plaintiffs' communications do not happen to go through the copied cables, switches, and routers.

SaltHill
STATISTICAL CONSULTING

ALAN J. SALZBERG, PH.D.
salzberg@salthillstatistics.com
646-461-6153

EXPERIENCE

Salt Hill Statistical Consulting, Founder and Principal, 2000-present
Founder and Principal of a statistical consulting company (formerly Quantitative Analysis). The firm is skilled at presenting complex ideas to non-experts. Capabilities include development and implementation of statistical techniques as well as critical review and audit of existing statistical estimates, samples, and models. The company's clients are law firms, government, and private corporations and have included: United States Department of Labor; Pfizer; Barnes & Thornburg; Honeywell; K&L Gates; City of New York

Summit Consulting, Teaming Partner, 2009-present
Consult on multiple engagements with economic consulting firm on large-scale government projects. Served as a Director at the firm in 2014.

Analysis & Inference, Inc., CEO, 1991-1995 and 2008-2013
Led a statistical consulting company that provides consulting services to corporations, law firms, and government.

KPMG LLP, Practice Leader, Quantitative Analysis Group – New York, 1996-2000
Established and led the New York office of KPMG's Quantitative Analysis Group. Built a consulting practice with annual revenues of $4 million.

Morgan Stanley, Associate, 1988-1990, 1995-1996
Performed statistical modeling and software design.

EDUCATION

Ph.D., Statistics, Wharton School, University of Pennsylvania, 1995
M.A., Statistics, Wharton School, University of Pennsylvania, 1992
B.S., Economics (concentration in Economics and Finance), *cum laude*, Wharton School, University of Pennsylvania, 1988

ENGAGEMENTS

- Served as a statistical consultant in the development of dynamic models for residential property valuation across the United States in order to determine whether certain residential mortgage-backed securities (RMBS) were fairly valued. Made use of statistical and econometric techniques including regression modeling, statistical sampling, bootstrapping, and bias adjustment.

- On behalf of a Fortune 100 company, evaluated models that estimated the potential liability in more than 10,000 asbestos settlements. In addition, reviewed the likely bias and other issues with a model that predicted the "propensity to sue" for future claims. Wrote two expert reports concerning findings and testified as a statistical expert regarding those findings.

- On behalf of the New York State Office of Medicaid Inspector General, reviewed the sampling and estimation methodology used to audit Medicaid providers in New York State. Reviewed and critiqued specific methodologies in ongoing matters, and provided recommendations for improving the statistical audit process.

- In a series of matters on behalf of the law department for a major city, created and analyzed a massive real estate database, modeled market and sales values, and wrote expert reports to determine potential biases of alternative methods of valuing commercial real estate. Determined the validity of assumptions about lease lengths, turnover rates, and other issues affecting rents and property values. Testified as a statistical expert in one of these matters.

- On behalf of the United States Department of Labor, acted as the principal investigator on a study of industry compliance with certain labor laws. Developed and pulled a statistical sample for evaluation. Performed survival analysis to better understand how long certain industry investigations would last and the likely outcomes of such investigations.

- For major pharmaceutical company, analyzed company and external marketing data to determine reliability and potential biases in using external data sources. Analyzed physician-specific data for a period of 36 months concerning product marketing to approximately 1 million prescription drug subscribers.

- In complex litigation matter involving an undersea oil field, analyzed data from several years of inspections and repairs to determine likelihood of a catastrophic failure that would result in a major oil spill. Used survival analysis to determine the likelihood of such an event for different inspection and repair cycles.

- On behalf of several state public service commissions, directed data analysis and statistical design in a series of tests of Bell South, Verizon, SBC-Ameritech, and Qwest. Beginning in 1998, developed software and procedures for calculating performance metrics and evaluating the competitive environment. Testified before several state public service commissions, including New York, Virginia, Florida, Michigan, and Colorado.

- Using social security and insurance company data, developed two probability-based models in order to match unclaimed assets with the individual owners of those assets. The models were successfully implemented at our client, a financial services company, and used to assist state agencies in locating unclaimed assets.

- For hedge fund, performing an ongoing series of projects related to pricing risk and return of various investment options. Using standard and proprietary statistical techniques and software, developing models to select appropriate investment funds according to risk and term of investment.

77 Water Street, 7th Floor • New York, NY 10005 • 646 461 6153 • salzberg@salthillstatistics.com
www.salthillstatistics.com

- For large direct market publisher, improved customer response modeling while reducing the costs of test marketing. Overall test marketing was reduced by combining data for various market segments. This method also increased the precision of the scores assigned to customers concerning their propensities to purchase individual books. These improvements were expected to lead to cost savings and revenue improvement totaling about $1 million annually.

- Modeled television audience ratings to determine the Public Broadcasting System's share of cable royalty distributions. Used statistical methods to determine a reliable estimate of PBS's cable royalty share. The estimate resulted in a multi-million dollar decision in favor of the Public Broadcasting System by the Cable Royalty Tribunal.

- Lead statistician in the design and implementation of a sample of all personal property and equipment on behalf of the United States Internal Revenue Service. The population of interest involved more than one million items contained in over 1,000 buildings. The sample design, implementation, and resulting estimates and projections were subject to intense scrutiny by the United States General Accounting Office.

- For the United States Department of Justice, designed and implemented a sample to estimate the number of immigrants improperly granted citizenship. The sample was designed to provide precision of plus or minus less than 1%, for a population of more than 1 million immigrants. The work was the focus of intense congressional scrutiny and received substantial review in the media.

- On behalf of Fortune 100 company, created statistical models to determine the probabilities and likely severities of accidents for different employee and accident types. This project resulted in recommended annual savings of $3 million.

- On behalf of the Arava Institute of Environmental Studies, advised on design and sampling methodology for a broad-based survey of environmental education in middle and high schools. More than 7,000 students were surveyed in a sample that was stratified by size of town, income level, and other socio-economic variables. Performed weighted statistical analysis to project survey results to the population. Presented results before Israeli Congressional committee in July 2007.

- For the United States Customs Service (Department of Homeland Security), assisted with sampling of financial statement information. Designed and wrote sampling plans, helped implement the plans, and created spreadsheet calculator to analyze results. In an earlier engagement, evaluated the credibility of statistical sampling and analysis used to track and categorize imports, for the Office of Inspector General. Suggested improved methods of sampling and implementation.

- Designed and implemented several studies of stock basis in corporate mergers. One universe comprised over 100 million shares and more than 20,000 shareholders, yet the sample design resulted in a highly precise estimate using data for fewer than 1,000 shareholders.

RESEARCH

77 Water Street, 7th Floor • New York, NY 10005 • 646 461 6153 • salzberg@salthillstatistics.com

www.salthillstatistics.com

An excerpt from my "What are the chances?" blog appears in Lundsford, Andrea L. and Ruszkiewicz, John, *Everything's an Argument, 6th Edition, 2012* and Lundsford, Andrea L., Ruszkiewicz, John, and Walters, Keith, *Everything's an Argument with Readings, 6th Edition, 2012*.

"Law and Statistics of Combining Categories: Wal-Mart and Employment Discrimination Cases", with Albert J. Lee, *Proceedings of the 2010 Joint Statistical Meetings of the American Statistical Association*, 2010.

"Evaluating the Environmental Literacy of Israeli Elementary and High School Students," with Maya Negev, Gonen Sagy, and Alon Tal, *Journal of Environmental Education*, Winter 2008.

"Trends in Environmental Education in Israel," with Gonen Sagy, Maya Negev, Yaakov Garb, and Alon Tal, *Studies in Natural Resources and Environment*, Vol. 6, 2008. [In Hebrew]

"Results from a Representative Sample in the Israeli Educational System," with Gonen Sagy, Maya Negev, Yaakov Garb, and Alon Tal, *Studies in Natural Resources and Environment*, Vol. 6, 2008. [In Hebrew]

"Comment on Local model uncertainty and incomplete-data bias by Copas and Li," with Paul R. Rosenbaum, *Journal of the Royal Statistical Society, Series B*, 2005.

"Determining Air Exchange Rates in Schools Using Carbon Dioxide Monitoring", with D. Salzberg and C. Fiegley, presented at the *American Industrial Hygiene Conference and Expo*, 2004.

"The Modified Z versus the Permutation Test in Third Party Telecommunications Testing", *Proceedings of the 2001 Joint Statistical Meetings of the American Statistical Association*.

"Removable Selection Bias in Quasi-experiments," *The American Statistician*, May 1999.

"Skewed oligomers and origins of replication," with S. Salzberg, A. Kervalage, and J. Tomb, *Gene*, Volume 217, Issue 1-2 (1998), pp. 57-67.

"Selection Bias in Quasi-experiments," (Doctoral Thesis), 1995.

***Patent** (#6,636,585)* One of five inventors on a patent for statistical process design related to information systems testing.

PRESENTATIONS

- Panelist and Presenter of "Secrets to Effective Communication for Statistical Consultants,", Joint Statistical Meetings of the American Statistical Association, 2013, with Ghement, Isabella; Mangeot, Colleen; Rantou, Elana; Schuenemeyer, Jack; and Turner, Ralph.

- Lectured on "Statistics in Predictive Coding" as part of a one day seminar sponsored by the Cowen Group and Equivio in the area of e-discovery, 2012.

77 Water Street, 7th Floor • New York, NY 10005 • 646 461 6153 • salzberg@salthillstatistics.com
www.salthillstatistics.com

- Presented paper (with Albert Lee) entitled "Law and Statistics of Combining Categories: Wal-Mart and Employment Discrimination Cases" at the Joint Statistical Meetings of the American Statistical Association, 2010.

- Delivered presentation on census data from the New York City Housing and Vacancy Survey, before the New York City Rent Guidelines Board, 2007.

- Part of a team of five presenting results before an Israeli congressional committee regarding a nationwide public school survey, 2007.

- Served on panel and presented "The Modified Z versus the Permutation Test in Third Party Telecommunications Testing" at the Joint Statistical Meetings of the American Statistical Association, 2001.

- Delivered talk regarding "Skewed oligomers and origins of replication" at Hebrew University in Jerusalem, 1999.

PERSONAL

Married, with two daughters and a son.
Languages: English (native), Hebrew (conversational).
Member, Park Slope Food Coop.
Member, 39 Plaza Housing Corp (residential coop). Board member, 2012-2015.
Enjoy ultimate Frisbee, basketball, biking, hiking, running, tennis, chess, and bridge.

77 Water Street, 7th Floor • New York, NY 10005 • 646 461 6153 • salzberg@salthillstatistics.com
www.salthillstatistics.com

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS; HUMAN RIGHTS WATCH; AMNESTY INTERNATIONAL USA; PEN AMERICAN CENTER; GLOBAL FUND FOR WOMEN; THE NATION MAGAZINE; THE RUTHERFORD INSTITUTE; and WASHINGTON OFFICE ON LATIN AMERICA,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE; ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE; JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; DEPARTMENT OF JUSTICE; and ERIC H. HOLDER, in his official capacity as Attorney General of the United States,

Defendants.

Hon. T. S. Ellis III

No. 15-cv-00662-TSE

DECLARATION OF ROBERT T. LEE

I, Robert Lee, do hereby state and declare as follows:

Introduction

1. I am an entrepreneur and consultant specializing in information security, incident response, and digital forensics. I am currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute; I also own a consulting firm. I have more than 15 years of experience in computer forensics, vulnerability, and

exploit discovery, intrusion detection/prevention, and incident response. I graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information warfare. Later, I was a member of the Air Force Office of Special Investigations (AFOSI) where I led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting my own firm, I directly worked with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber-forensics branch, and lead for a computer forensic and security software development team. I was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for four years prior to starting my own business. I have also co-authored the book *Know Your Enemy*, 2nd Edition and MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat. I earned an MBA from Georgetown University in Washington DC.

2. The purpose of this declaration is to provide a basic explanation of the process by which Internet users typically view or download information available on a website, including the way information travels through the high-capacity fiber optic cables comprising the Internet "backbone." This declaration also explains that, as a technical matter, it would not be necessary to copy all information on a given "backbone" cable in order to copy information traversing one or more of the sub-cables within that backbone cable. With respect to identifying Internet users, this declaration explains that it is difficult to identify an individual user based on the information that is typically transmitted when a user

views a website; indeed, as discussed below, when users visit websites to view or download information, the operators of those sites generally do not obtain the individual users' identities unless the users themselves provide (or have provided) that information. Finally, in this declaration I also address various types of communications traffic carried on the Internet, and the comparatively small share of that Internet traffic that may be attributed to requests for information on websites operated by Wikimedia Foundation.

The Internet, Internet Service Providers, and Internet Protocol

3. A group of two or more computers linked together to permit communication among them make up a network. Networks connected by intermediate devices that route information between them become an internetwork. The biggest internetwork is the Internet, the global communications network that allows computer networks worldwide to connect and exchange information.[1]

4. Users may engage in many activities on the Internet such as web browsing, sending and receiving e-mails, instant messaging, video conferencing (such as through Facetime and Skype), and video streaming. Web browsing, by way of example, involves access to the World Wide Web. The Web is a branch of the Internet, a system of computers housing a collection of publicly accessible documents (including text documents, images, audio and video files, etc.). A user accesses the World Wide Web through a "browser," such as Internet Explorer or Google Chrome, which runs on the user's computer, smartphone, or other device.

---

[1] In contrast, an *intranet* is a computer network internal to an organization that is frequently not connected to the Internet, or is connected to the Internet through a "firewall," a network security system that blocks unauthorized incoming traffic while permitting outward communication.

5. To communicate over the Internet (and therefore with the Web) a user must obtain a connection from an Internet Service Provider ("ISP"). Typically an ISP is a private company that provides a subscriber access to the Internet for a periodic fee. Subscribers to an ISP's services can be individuals, businesses, educational institutions, government agencies, or other organizations. Access can be provided by the old telephone copper wire, fiber-optic cable, coaxial cable, other types of data lines, or wireless satellite signal to the subscriber's home, place of business, or wherever the subscriber's device is physically present. Typically, in a setting such as a home or business, the connection is made through a device located at the subscriber's home or place of business (and often supplied by the ISP) called a router[2] or modem. (If a subscriber is connecting to the Internet via the network associated with a smartphone, then access is provided through the cellular telephone network.) ISPs vary in size and the range of services provided, from nationwide providers such as Verizon and Comcast to much smaller regional and local providers.

6. To communicate with one another and exchange information, devices connected to the Internet follow a set of rules or protocols referred to as the "Transport Control Protocol/Internet Protocol" ("TCP/IP"). That set of standards facilitates communication between different computers or networks of computers. Among other things, it establishes rules for breaking communications into "packets" that can travel efficiently; addressing packets to the correct destinations; and providing for quality control to confirm that communications arrive undamaged at their intended destinations.

---

[2] Routers are used to connect networks to other networks, and as I explain below, data traveling over the Internet will pass through multiple (sometimes dozens of) routers before reaching its destination.

7. Following these protocols, a computer sending information on the Internet will divide that data into packets typically compromised of 600-1,500 bytes and add layers of header information, including: the IP address (described in paragraph 9 below) of the recipient and the sender; and a calculation that allows the destination computer receiving the packet to determine whether the data was damaged during transmission and needs to be resent.

8. Each packet will also include information that could be stripped out and replaced by any number of "intermediate nodes" (devices that forward that packet on its way to its ultimate destination). Depending upon the path the packets travel, that process of removing and adding new information may be repeated many times.[3]

How Information Travels over the Internet

9. As noted above, rather than physical addressing, TCP/IP networks, including the Internet, use Internet Protocol ("IP") addressing to send and deliver information. An IP address is a unique numeric string, such as 149.101.146.71 (the IP address of the Department of Justice website), that identifies one computer or other device to other computers or devices on a network or internetwork. When, for example, the user of one device seeks to retrieve information contained on another, the IP addresses allow the global

[3] While each TCP packet includes substantial addressing and other technical information, which is necessary to facilitate the travel of the packet from the user to its destination, each packet of data, or even all of the packets associated with a single communication, do not reflect the technical infrastructure of a sender's or recipient's computer or computer network or data flows. Instead, to begin to reconstruct the technical infrastructure supporting a particular website on the Internet, for example, substantially all of the traffic flowing to and from that website's servers would need to be recorded, ingested into a database, and then, most importantly, analyzed to try to piece together the infrastructure and data flows involved. Even then, aggregating all of that information would, at most, create a picture of the website or servers that have received public IP assignments (discussed in paragraphs 15 and 16 below); mapping out the private and internal infrastructure supporting that website would still be difficult, if not impossible, to achieve.

communications network to route the user's request to the second device, and then to route the response from the second device, containing the requested information, back to the user's device. In this way, IP addresses act like the sender and recipient addresses on mail carried by the U.S. Postal Service (although IP addresses contain less identifying information than the outside of an envelope in the mail).

10. While the process usually is not apparent to the user, information being sent from one device to another can travel through numerous other networks and traverse multiple intermediate nodes en route to its destination. Dedicated computers known as "routers" receive information from other nearby routers around them and determine the best path for information to follow in traveling from the user's device to its ultimate destination. Because there are numerous paths information may take when traveling between two points on the Internet, routers may select a pathway based on factors such as cost, distance, speed, and reliability.

11. If the information is traveling to a destination outside of the user's regional network, a router can send it (likely through other intermediate routers) to a "network access point" where the information will flow onto the internet "backbone," a network of high-capacity (typically) fiber-optic cables maintained by the large or "Tier 1" ISPs. The backbone includes terrestrial fiber-optic cables, as well as submarine fiber-optic cables. Every such modern fiber-optic cable, in turn, consists of multiple smaller sub-cables housed inside that can each contain up to one thousand silica glass fibers. Data transmitted on the Internet backbone travel those glass fibers in the form of optical signals, or pulses of light.

12. Generally, all of the packets comprising a single communication travel on the same single hair-thin glass fiber. When information is broken into packets pursuant to the TCP/IP protocol described above, it is possible, but unlikely, that routers will direct the packets to different paths. Typically, the packets of one communication will be separated and sent on different paths only if a change in conditions—such as a suddenly high volume of traffic on the initial path—renders a different path more advantageous than the route initially selected.

13. Because the packets constituting a single communication are likely to travel on the same fiber within a sub-cable of a backbone cable, it would not be necessary, *as a technical matter*, to copy the entire stream of communications carried on every fiber within a sub-cable of a backbone cable to be reasonably certain of obtaining all of the packets constituting a specific communication.[4] Furthermore, it would not be necessary, *as a technical matter*, to copy all the streams of communications on an entire backbone cable in order to copy all of the communications traveling across a particular sub-cable within that backbone cable.[5]

---

[4] Moreover, not all packets of a given TCP stream are necessary to intelligibly assemble its contents. In addition to those packets delivering the content of the information being sent and received, each TCP stream includes packets that do not transmit substantive information but that facilitate the connection. For example, each TCP stream begins with a "three way handshake," a request to open a connection, acknowledgment by the recipient of that request, and one more acknowledgement that the second transmission has been received by the device that initiated the connection. Additional packets not responsible for transmitting the substance of the data the user is sending—for example additional acknowledgements—are sent while the TCP connection remains active, and, after the transmission of substantive information is complete, additional packets are sent to close the connection.

[5] I want to emphasize here that I have no knowledge of how the NSA conducts the surveillance at issue in this case. My point here is simply that, as a matter of technology, copying information transmitted on one sub-cable of a backbone cable does not require copying all information transmitted on every sub-cable within that particular backbone cable.

14. Although the packets of a single TCP stream—the multiple packets of data comprising a single communication—are likely to be routed along the same path, distinct communications may follow different routes to reach their respective destinations, even if they are being sent from the same region of the world (or even the same country) to the same region of the United States. For example, two different communications being sent to the same country may travel on different fibers within the same sub-cable, or may even travel on different submarine cables altogether. Their respective routes will be determined by the routers their respective TCP streams encounter based on the factors discussed above (including cost, distance, speed, and reliability).

Public IP Addresses

15. IP addresses used for communication across the Internet are called public IP addresses. Public IP addresses are assigned to Internet subscribers by their ISPs. An ISP may assign a subscriber a static public IP address or dynamic public IP addresses. A static public IP address is one assigned to a subscriber on a long-term basis, in much the same way that a telecommunications company assigns telephone numbers to its subscribers. Dynamic public IP addresses, in contrast, are assigned to subscribers on a more intermittent basis—whether for a day, an hour, or some other period of time, depending on the needs, resources, and practices of a particular ISP—after which they are assigned to other subscribers. By way of example, if an ISP assigns a particular public IP address to a subscriber only for a specific length of time while the subscriber is connected to the Internet, then the IP address is assigned when the subscriber (or someone else making use of the subscriber's service) connects to the Internet, and may then be released and available to another subscriber when that period of time ends. Thus, the same public IP

address may be used by numerous subscribers on the same day, or reassigned from subscriber to subscriber from one day to the next.

16. Web browsing, like other user activities conducted on the Internet, depends on public IP addressing. Websites usually consist of information contained on multiple webpages (for ease of organization, review, and downloading), and are hosted on one or more computers with assigned public IP addresses. When a user accesses the Internet, through a connection provided by an ISP, in order to read, download (or, if permitted, to edit) the contents of a website, a request is sent from the user's device. That request is associated with and contains a public IP address that was assigned by the ISP. Pursuant to the protocol described above, the user's computer will add header and footer information to the request, including the public IP address assigned by the ISP, and may break the request into packets. That stream of packets is then routed to the public IP address assigned to the website.

17. When the user's request to view or download content arrives at the website, the website's host computer(s) automatically generate a return message that includes the requested information, together with the public IP address associated with the request from the user's device, so that the information may be routed, through the ISP, back to the requesting user.

18. To allow the user to view a requested webpage (a specific page that is part of a website), the website's host computers send the files comprising that webpage to the user's device. A webpage, however, may consist of many (even hundreds of) files. The number of files comprising a webpage depends on the complexity of that webpage's content. The text appearing on a webpage, for example, constitutes a different file from any banners or

images on that webpage; any banners or images are each stored as separate files that may reside on different servers. Thus, to allow a user to view a webpage containing fifteen graphics, the webpage's host computer (or computers) would send sixteen files to the user's computer—one file to convey the text, and fifteen files to convey each of the images appearing on that page.[6] The host computer's log could reflect sixteen hypertext transfer protocol ("HTTP") "requests"[7] for that single page view. The higher number of ads and graphics a website has, like Facebook.com or cnn.com, the more "requests" would be logged for a single webpage view; in contrast, a website with no ads and fewer images, such as the websites of Wikipedia.com, the fewer "requests" logged for each single webpage view.[8]

19. During this fully automated process, the routers along the global communications network rely on the public IP addresses associated with the user's request, and the website's host computers, in order to facilitate the transfer of the information via the Internet.

---

[6] To make the journey to the user's device, each of those files would again be broken up into TCP/IP packets, as described in paragraphs 6–7. Upon arrival at the user's device, the packets would be reassembled by the user's device into graphics or text, and then graphics or text would be used to display the complete webpage the user had requested.

[7] If that communication stream were encrypted, those "requests" would be referred to as hypertext transfer protocol secure ("HTTPS") "requests."

[8] HTTP/S "requests" or "hits" help measure how many files a server sends and receives, and thus how much traffic that server handles, but they are not a reliable metric for determining the comparative popularity and usage of websites. For example, depending on the number of advertisements and graphics on two webpages, a request to view the content of one webpage with no ads and only a few graphics would result in only a handful of HTTP requests, whereas a single request to view the content of another webpage containing many ads and graphics can generate multiple, or even hundreds of HTTP requests. In this way, counting HTTP requests can be a misleading indicator of how many webpages are being viewed.

20. At no time during this process is the individual using a device to obtain information from a website (or to provide information to a website, as the case may be) identified by name or other personally identifying information unless that user has specifically provided that information to the site in some way. (For example, a user may provide identifying information, such as name, address, and credit card number to purchase an item from a website; that information may be sent in the request to the website, or the user may have previously supplied such information to the site.) When simply viewing or downloading the contents of a website, in contrast, the request or message sent from the user to the website's host computer contains no such personally identifying information. The request or message does contain a public IP address assigned by an ISP, however. The ISP that assigned the IP address, be it static or dynamic, may review its logs to identify the subscribing individual (who may be different than the user) or organization to which the public IP address was assigned at the moment the user's message was sent.[9] But that identifying information is not transmitted to or from the website's host computers when a user views, downloads, or edits a website.

21. In short, when a user simply reads or downloads content from a website, the operators of that site know the public IP address, assigned by an ISP, that is associated with the particular request from that user's device—but not the identity of the user. Moreover, the public IP addresses associated with future requests by the same user may change depending on when or where the user makes those requests, even if the requester uses the

[9] Indeed, a user also may hide the public IP address by subscribing to (or obtaining for free) an anonymizing service such as www.the-cloak.com, www.anonymouse.com, or www.proxify.com. If the user subscribed to one of these services, the public IP address forwarded to the website's server would be one obtained on loan from the service and not the public IP address assigned by the ISP providing the connection to the Internet.

same device. The following examples illustrate these points in a variety of conventional circumstances:

a. An individual located in a residence connects to the Internet via the homeowner's ISP. This person may be the homeowner, or a family member, using the homeowner's personal computer. Or the individual may be a visitor using his or her own laptop computer or tablet who connects through the owner's home Wi-Fi network. The public IP address associated with any request or other message sent by this individual, whether the homeowner, a family member, or a visitor, will be a static or dynamic public IP address assigned to the homeowner-subscriber at that time by the ISP.

b. An individual located at his or her place of employment may connect to the Internet through the employer's ISP using a desktop computer provided by the employer. The public IP address associated with any requests or messages sent by the employee will be a public IP address assigned to the employer by the employer's ISP, and the next day, hour, or even moment, requests or messages from other individuals working for the same employer may be associated with the same public IP address.

c. In much the same way, a student located at a university dorm or library may use his or her own laptop or tablet computer to connect to the Internet, through the university's Wi-Fi wireless network, via the university's ISP. The public IP address associated with the student's online communications will be one assigned by the ISP to the university, not the individual student, and, for example, may later be associated with other students' communications when they access the Internet through the university's Wi-Fi wireless network.

d. Customers using laptops or tablets to access the Internet through public Wi-Fi service provided at an Internet café, or a Starbucks, connect to the Internet through the ISP to whose service the Starbucks subscribes. The online requests and other communications of a Starbucks customer will be associated with a public IP address from among those assigned to the Starbucks by its ISP. If later that day the same customer connects to the Internet using the Wi-Fi service at a McDonald's, his or her communications, even though made on the same laptop or tablet computer, will be associated with a different public IP address from among those allocated to the McDonald's by its own ISP.

e. When a user seeks to access content from a website using a smart phone, her request is first routed via the cellular telephone network to her ISP (which is likely also her cellphone service provider). The ISP assigns a public IP address to the request and forwards it for routing over the Internet to the desired website. The address may be a dynamic public IP address assigned to the user's communications only for the duration of a particular Internet session. Moreover, depending on the needs, resources, and practices of the user's ISP, and because each ISP only has a finite block of public IP addresses that it may assign, the ISP may choose to simultaneously assign the same public IP address to multiple requests from different cellphone subscribers connected to the Internet at the same time. The ISP would then use internal identifiers (such as a user's cellphone number, IMEI number, or port number) to route return communications to the appropriate user's device. None of these internal identifiers are included, however, in a user's request sent to a website and so cannot be used by the website to identify the individual user as the originator of the request.

22. The above examples illustrate that, even when the IP address associated with a particular request to view a webpage is known, it is often difficult, and certainly not a trivial matter, to identify the subscriber associated with the public IP address, let alone the individual user who sent the request.[10] If a person or entity knows a public IP address, one can use a website such as http://mxtoolbox.com/ReverseLookup.aspx, to find out the ISP that assigned that public IP address. But ISPs typically do not provide such information except in response to legal process like a subpoena. If the ISP is foreign-based, rather than domestic, securing the ISP's cooperation in response to legal process is more difficult and could present an insurmountable obstacle to identifying the subscriber. And,

---

[10] Additional information that could be transmitted in a user's interaction with a website (for example log-in credentials, information that can be used to show prior approximate geolocation, and information about the model of the device making the request) could be used only in conjunction with other investigative techniques to determine the identity of an otherwise anonymous user. For example, it would be difficult to link log-in credentials with a specific individual without conducting a forensic investigation of the user's devices or having the individual himself acknowledge that that was his log-in information. Similarly, approximate geolocation and information about the device sending the request would not identify an individual user as having sent a specific communication. Such information would help narrow the inquiry to a specific region, or to persons who have access to a specific type of device, but additional forensic or other investigation would be required to identify the individual who sent a specific communication.

as the examples above show, identifying the subscriber is not necessarily the same as identifying the user. In the example of the Starbucks or McDonald's customer using the Wi-Fi wireless network, an ISP, responding to appropriate legal process, could identify the subscriber (Starbucks or McDonald's), but thereafter identifying the user who accessed a particular website through the Wi-Fi connection will depend on whether those corporate subscribers maintain a log of usage and for how long. In many cases, identifying an individual user who made a particular communication—when only the public IP address associated with that communication is known—can be a difficult matter.

23. I have read the Privacy policy posted by the Wikimedia Foundation at http://wikimediafoundation.org/wiki/Privacy_policy.[11] In that policy, Wikimedia informs individuals who read, contribute to, or edit information on its websites (whom it calls its "users") that it may acquire certain information automatically when a user accesses one of Wikimedia's websites. The policy indicates that this information includes the type of device used, the user's language preference, and perhaps the name of the Internet Service Provider. Additionally, the privacy policy states that various Wikimedia websites may also automatically and "actively collect some types of information with a variety of commonly-used technologies." The policy indicates that these technologies include "cookies" and "tracking pixels." A cookie is a small amount of data generated by a website that is stored on the user's device if the user's device is configured to allow the storage of cookies. Cookies may be used (for example) to store user login information and preferences, such as language preference. Tracking pixels are snippets of code that

[11] Exhibit A: Privacy policy - Wikimedia Foundation.pdf

allow a website to track how a user interacts with the website (for example, which pages a user views and for how long). The information that Wikimedia automatically collects about its users, as indicated in its privacy policy, does not individually identify specific users.

Wikimedia Users and Communications in the Context of Total Internet Usage

24. It is important in any discussion of the numbers of website "communications" to put that discussion into the context of global Internet usage. In the computer and related network technologies field, as with other professions, we look to and rely upon the best available statistical data sources. Regarding communications traffic on the Internet, there are various information technology and market research organizations that compile data upon which a person in the field may rely to understand the magnitude of the numbers involved. Paragraphs 24-34 of this declaration are based on reliable and publicly available data that I was able to locate for purposes of the declaration.

25. In terms of Internet users, various sources agree that there are now approximately 3.0 billion Internet users worldwide. *See* http://www.internetlivestats.com[12] (last visited, July 30, 2015) (3.130 billion); http://www.internetworldstats.com/stats.htm[13] (last visited July 30, 2015) (3.079 billion Internet users worldwide); Internet Society, Global Internet Report 2014,

https://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf,[14] at 7, 19 (noting there were 2.893 billion Internet users in May 2014; estimating the number of users would exceed 3.0 billion by early 2015).

---

[12] Exhibit B: Internet Live Stats - Internet Usage & Social Media Statistics 10_30 pm.pdf

[13] Exhibit C: World Internet Users Statistics and 2014 World Population Stats.pdf

[14] Exhibit D: Global_Internet_Report_2014_0.pdf

26. In terms of the volume of Internet traffic, Cisco, a worldwide leader in Information Technologies, reports that, whereas in 1992 global Internet traffic consisted of 100 gigabytes of information per day, in 2012 the same traffic reached 12,000 gigabytes of information per second. *See* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html,[15] at 5-6; *see also* http://www.internetlivestats.com (last visited July 30, 2015) (Exhibit B) (tabulating the Internet traffic for July 30, 2015 alone as 2.4 billion gigabytes as of 11:00 p.m. and 28,777 gigabytes per second). This traffic consists of a variety of communications and other Internet activity, including email, web browsing, social media, audio and video streaming, Voice Over Internet Protocol (VOIP) (Internet telephony), video conferencing, and peer-to-peer sharing of information. Video traffic comprises 66% of the total Internet traffic and is estimated by Cisco to be 79% by 2018. Exhibit E, at 3; *see also* Internet Society, Global Internet Report 2014, https://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf, at 7, 21 (in 2012, video was 50% of Internet traffic).

27. E-mails are one example of text-based communications that transit the Internet. According to The Radicati Group, Inc., a technology market research firm, 182.9 billion emails were sent *per day* in 2013, that is, approximately 5.48 trillion emails per month. *See* http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-

---

[15] Exhibit E: The Zettabyte Era—Trends and Analysis - Cisco.pdf

2013-2017-Executive-Summary.pdf,[16] at 4; *see also* Internet 2012 in numbers in Tech Blog (Jan. 16, 2013), http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/[17] (relying on the Radicati Group's number of 144 billion mails sent worldwide every day in 2012). The figures reported by the Radicati Group are consistent with the 207 billion emails sent on July 30, 2015 as of 11:00 p.m.,[18] as reported by http://www.internetlivestats.com (last visited July 30, 2015) (Exhibit B).

28. Using the current figure of 207 billion emails per day, this corresponds to about 6.21 trillion emails per month and about 75 trillion per year. Accordingly, Wikimedia's claimed 21.25 billion monthly page views by its users[19] corresponds to less than fourth-tenths of one percent (0.34%) of just the monthly e-mail traffic carried on the Internet, and would represent a much smaller fraction of the total traffic carried on the Internet each month.[20]

---

[16] Exhibit F: Email-Statistics-Report-2013-2017-Executive-Summary.pdf

[17] Exhibit G: Internet 2012 in numbers _ Pingdom Royal.pdf

[18] Assuming a month with 30 days, these 207 billion emails per day equate to about 6.2 trillion per month.

[19] In paragraph 87 of their First Amendment Complaint, Plaintiffs assert that from April 1, 2014 to March 31, 2015, Wikimedia websites received over 255 billion webpage views. Assuming an even distribution over each month, that equals about 21.25 billion webpage views per month.

[20] Tweets are another example of text-based communications that transit the Internet. According to Twitter, there were approximately 500 million tweets per day in 2013 (or 5,700 tweets per second) with an average growth of 30% per year. *See* Exhibit H: Krikorian, Raffi (VP Twitter Platform Engineering, Twitter, Inc.), https://blog.twitter.com/2013/new-tweets-per-second-record-and-how. Based on this annual rate of growth, the number of tweets per day in 2015 would be in the range of 850 million. This estimate is consistent with the 805 million tweets tabulated for July 30, 2015 alone as of 11:00 p.m., http://www.internetlivestats.com (last visited July 30, 2015) (Exhibit B), which corresponds to approximately 24.1 billion tweets per month or 293 billion year.

29. Web browsing is another component of Internet traffic. There are currently about 978 million websites, http://www.internetlivestats.com (last visited July 30, 2015) (Exhibit B), down from over 1.0 billion in 2014, *see* http://news.netcraft.com/archives/2014/10/10/october-2014-web-server-survey.html[21]; Internet Society, Global Internet Report 2014 at 24, https://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf (Exhibit D). Although, according to Internet Live Stats, about 75% of these websites may be inactive, *see* http://www.internetlivestats.com/total-number-of-websites[22] (last visited July 30, 2015), that still means there are approximately 244 million active websites.

30. Certain commercial organizations track website usage on these websites. Alexa, a well-known company that provides commercial web tracking data, ranks the top one million websites. *See* https://support.alexa.com/hc/en-us/articles/200449834-Does-Alexa-have-a-list-of-its-top-ranked-websites[23]. Wikipedia.org, Wikimedia's top-ranked site, is ranked number 7, behind Google.com (1), Facebook.com (2), Youtube.com (3), Baidu.com (4), Yahoo.com (5), and amazon.com (6). *See* http://www.alexa.com/topsites[24] (last visited July 30, 2015). Another well-known website traffic checker, Similar Web, posts its

[21] Exhibit I: October 2014 Web Server Survey _ Netcraft.pdf

[22] Exhibit J: Total number of Websites - Internet Live Stats.pdf

[23] Exhibit K: Does Alexa have a list of its top-ranked websites_ – Alexa Support.pdf

[24] Exhibit L: Alexa Top 500 Global Sites.pdf

rankings as well as the number of website visits and the average webpage-views per visit. *See* http://www.similarweb.com[25] (last visited July 30, 2015).

31. Similar Web posts a list of the top 50 websites on the publicly available portion of its website. *See* http://www.similarweb.com/global (last visited July 30, 2015).[26] In Similar Web's rankings, Wikipedia is globally ranked as the number eight website, whereas it is ranked as number seven in Alexa's rankings; Wikipedia.org is ranked number 10 by Similar Web in the U.S. *See* http://www.similarweb.com/website/wikipedia.org[27] (last visited July 30, 2015). Similar Web estimates that Wikipedia (a project of Wikimedia) had 2.4 billion visits in June 2015 with an average of 3.3 page views per visit, which means that there were approximately 7.92 billion (2.4 X 3.3) web page views for Wikipedia (not all Wikimedia projects) in June 2015. Facebook.com is ranked (by Similar Web) number one in the world (and number two in the U.S.) with an estimated 20 billion visits in June of 2015 and an average of 17.73 page views per visit, equating to approximately 354 billion (20 X 17.73) web page views per month. *See* http://www.similarweb.com/website/facebook.com[28] (last visited July 30, 2015). Google.com is globally ranked by Similar Web as number two (and number one in the U.S.) with an estimated 16 billion visits in June 2015, and an average of 12.97 page views per visit, amounting to approximately 208 billion (16 X 12.97) page views for that

---

[25] Exhibit M: Website Traffic & Mobile App Analytics _ SimilarWeb.pdf

[26] Exhibit N: Similar Web Global Rankings.pdf

[27] Exhibit O: Wikipedia-SimilarWeb.pdf

[28] Exhibit P: Facebook - similarweb.pdf

month. *See* http://www.similarweb.com/website/google.com[29] (last visited July 30, 2015).[30] Youtube, which is ranked number three by Similar Web (globally and in the U.S.), had an estimated 14.9 billion visits in June 2015 and an average of 10.02 page views per visit, which is to say approximately 149 billion (14.9 X 10.02) page views that month. *See* http://www.similarweb.com/website/youtube.com[31] (last visited July 30, 2015).[32]

32. The spreadsheet attached to this declaration as Exhibit T (with supporting documentation obtained from Similar Web) shows the number of monthly page views for the top 50 websites as reported by Similar Web.[33] (The page views are calculated as in paragraph 31, above, by multiplying the number of visits to the site by the average number of page views per visit.) As the spreadsheet shows, the page views on these top 50 websites total approximately 1.17 trillion per month (or 14.0 trillion page views per year). According to Wikimedia, the monthly volume of page views on its websites is 21.25 billion, which is just 1.8% of the monthly page views of these top 50 sites. And, of course,

---

[29] Exhibit Q: Google - similarweb.pdf

[30] Additionally, there were 4.13 billion Google searches (as opposed to using Gmail by signing on to Google.com or other uses of Google.com) on July 30, 2015, alone, as of 11:00 p.m. *See* http://www.internetlivestats.com (last visited July 30, 2015 (Exhibit B). And Google itself reports that there were 1.2 trillion searches in Google in 2012 (or 100 billion searches per month). *See* http://www.google.com/zeitgeist/2012/#the-world), Exhibit R: Zeitgeist 2012 – Google.pdf).

[31] Exhibit S: Youtube-similarweb.pdf

[32] Using a different metric, there were 8.7 billion Youtube videos watched on July 30, 2015, alone, as of 11:00 p.m., which is approximately 261 billion per month. *See* http://www.internetlivestats.com (last visited, July 30, 2015) (Exhibit B).

[33] Exhibit T: Excel Spreadsheet of Top 50 Global Websites Per Similar Web (with attachments).

Wikimedia's monthly page views would amount to an even smaller percentage of the total monthly page views on the approximately 244 million currently active websites.[34]

33. When combined, the 1.17 trillion monthly page views on the top 50 websites and the 6.21 trillion monthly emails total 7.38 trillion online communications each month. The monthly volume of page views on Wikimedia's websites, 21.25 billion, is less than three-tenths of one percent (0.29%) of these 7.38 trillion communications alone.

34. In sum, to be properly understood, any figures purporting to quantify website users or webpage views must be placed in the context of global Internet usage and the volume of other global Internet traffic. Comparing the number of Wikimedia's international communications to the total volume of global Internet traffic reveals that Wikimedia's share of that traffic is comparatively small.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: August 5, 2015

ROBERT T. LEE

[34] As I noted earlier in paragraph 18, the number of webpage views is a more reliable indicator of website usage than the number of HTTP requests sent to or from a server used by a particular website. Wikimedia asserts that it received over 88 billion HTTP requests in May 2015. Regardless of whether that number is correct, it must be considered in context. The same metric could be used to measure the traffic on a top-ranked website like Facebook.com. Each time a user asks to view a webpage on Facebook.com, for example, the request will require multiple, and perhaps even hundreds, of HTTP requests because each ad and graphic will require separate HTTP requests. The more advertisements and graphics a webpage has the more HTTP requests will be necessary to view that page. Typically, therefore, a single page view on a site like Facebook.com, which contains many graphics and advertisements, will require many more HTTP requests than a page view on a text-heavy site, like Wikipedia, with few graphics and no ads. Therefore, if HTTP requests were used as the measure of a website's traffic instead of page views, then the volume of Wikimedia's communications would be even smaller in relation to sites like Facebook than if page views were used as the basis of comparison.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

WIKIMEDIA FOUNDATION, et al, Plaintiff,	)
v.	) CIVIL ACTION
NSA/CSS	) 1:15-cv-662
Defendants.	)

REPORTER'S TRANSCRIPT

MOTION HEARING

Friday, September 25, 2015

BEFORE: THE HONORABLE T.S. ELLIS, III
Presiding

APPEARANCES: PATRICK TOOMEY, ESQ.
JAMEEL JAFFER, ESQ.
ASHLEY GORSKI, ESQ.
ALEX ABDO, ESQ
DAVID ROCAH, ESQ.
DEBORAH JEON, ESQ.
American Civil Liberties Union
Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400

For the Plaintiffs

MICHAEL A. RODRIQUEZ, RPR/CM/RMR
Official Court Reporter
USDC, Eastern District of Virginia
Alexandria, Virginia

APPEARANCES (Continued)

RODNEY PATTON, ESQ.
JAMES GILLIGAN, ESQ.
JULIA BERMAN, ESQ.
CAROLINE ANDERSON, ESQ.
U.S. Department of Justice
Civil Division
Room 6102
20 Massachusetts Avenue N.W.
Washington, DC 20001

For the Defendant

THE CLERK: Wikimedia Foundation, et al versus NSA/CSS, et al.

Civil case number 1:15-cv-662.

THE COURT: All right.

Who is here on behalf of the various plaintiffs in this case?

Why don't we begin with the counsel who is, probably, by agreement and designated to take the leading role on this argument on the standing issue, who will that be?

ATTORNEY TOOMEY: That is me, your Honor.

Good afternoon. My name is Patrick Toomey. I am here from ACLU representing the plaintiffs.

If you would like me to introduce my colleagues, I can do that.

THE COURT: Yes, you may do so.

ATTORNEY TOOMEY: Also here with me from the ACLU are Jameel Jaffer, Alex Abdo, and Ashley Gorski.

ATTORNEY GORSKI: Good morning, your Honor.

ATTORNEY TOOMEY: And just so your Honor knows, our colleagues from the ACLU, Maryland, Deborah Jeon and David Rocah, who are also -- have appeared in the case are in the galley.

THE COURT: All right. What about all the other -- good morning to all of you or good afternoon now.

What about all the other plaintiffs?

ATTORNEY TOOMEY: We represent all the plaintiffs, your Honor.

THE COURT: All the plaintiffs.

ATTORNEY TOOMEY: Yes.

THE COURT: Okay. Thank you.

Now, for the government?

ATTORNEY PATTON: Good afternoon, your Honor.

Rodney Patton. I represent the NSA and all of the other defendants. I am from the Department of Justice.

Also with me at counsel table is James Gilligan, from the Department of Justice; Julia Berman, from the Department of Justice; and Caroline Anderson, from the Department of Justice.

THE COURT: All right.

Good afternoon to all of you.

And you are from the Programs Branch?

ATTORNEY PATTON: That is correct, Your Honor.

THE COURT: All right.

Let me ask Mr. Toomey. I just am serious. It has nothing to do with the case. Do you have a much older relative that was a student in England about 40 years ago, 45 years ago?

ATTORNEY TOOMEY: Not that I know of, your Honor.

THE COURT: All right.

ATTORNEY TOOMEY: I was a student briefly there, but I don't think that timeframe.

THE COURT: Well, I knew a student when I was a student there by the name of Dan Toomey, and that's not a relation?

ATTORNEY TOOMEY: I have several relatives name Dan Toomey, but I don't believe any of them were there with you.

THE COURT: All right.

Well, having covered my lack of any conflict on that side, let me point out that I think one of the leading lights of the Programs Branch is Ms. Jennifer Ricketts, who was my second group of law clerks some 30 years ago.

But that doesn't create a conflict, as far as I am concerned, but I disclosed it. I hope she is doing well.

ATTORNEY PATTON: She is doing very well, your Honor. Thank you for asking.

THE COURT: In fact, I have had a parade of clerks go through the Programs Branch. I don't even know how many of them are still even there. But I think most of them have gone -- passed on that way.

I say "passed on" because I am eager to share this. Recently a story appeared in a publication expressing some disagreement with an opinion I had written. That's not surprising.

But at published a picture of me, purporting to me be with that story. The picture was of a person I knew, liked, and admired, but it wasn't me.

It was a picture of Ed Becker, a judge of the Third Circuit who past away in 2006.

Rumors of my passing are greatly exaggerated as Twain said. But am delighted to be associated with Ed Becker, even in death. He was a very interesting, remarkable, and very funny man, always.

I recall once that he wrote an opinion entirely in verse. I didn't read it. But many people did. Poetry was never one of my loves.

All right. This is a -- you all have filed -- forests have died for what you all have done. It's a very interesting case.

Let me hear first from the defendant. I have some questions to ask you. You are the movant in this matter. And, so, it is your burden to persuade me.

This -- first of all, I want to thank every one for agreeing this to hear this in Alexandria. This case was, initially, filed in Maryland; and, for reasons that I have disclosed to you, it was -- couldn't be heard -- well, it could be heard there, but not by a Maryland judge.

And when I was asked to take the case, I communicated with counsel, and I am pleased to say that you agreed to have this motion heard here, which is convenient for me, and I hope not too inconvenient for you.

Actually, one of your clients, or one of the parties lives close to where I live. I don't know the man. But I live near Charlottesville, Virginia. And I think Rutherford does as well.

But, in any event, I appreciate the agreement of counsel to do this here. And to the extent that we do other things in this case, it will always be here if by agreement. If not, then we will go to Greenbelt.

Any counsel can raise an objection at any time, and I'll go to Greenbelt. Rather not, but it wouldn't be the first time I had to do something I didn't want to do.

Now, let me ask you a couple of initial

questions. First, this is a case that challenges the NSA's gathering of Internet data from communications.

It strikes me, in my occasional forays into reading newspapers, other than the sports page, which isn't often, that there have been a lot of these cases around, and I am not so happy about doing over what other people are doing.

Now, I am familiar with the D.C. Circuit case, of course, and I am familiar with the Second Circuit case, and with the Clapper case, and the Supreme Court, all of which you all have talked about at great length in your briefs.

But aren't there some other cases going on in district courts around the country right now?

ATTORNEY PATTON: Your Honor, as an initial matter, some of the cases that you referenced there dealt with bulk telephony metadata program.

THE COURT: Oh, I know it's not the exact same case.

ATTORNEY PATTON: So, it's not the exact same program; and that is, obviously, very important in terms of standing.

THE COURT: Yes, I understand that.

ATTORNEY PATTON: But there are, in fact --

THE COURT: All right.

Let me narrow it down to this. Are there any ongoing cases involving a challenge to the upstream collection of Internet data by the NSA?

ATTORNEY PATTON: Yes, there are -- there is, your Honor. At least one in the Northern District of California. We were counsel in that case, too.

The case went to summary judgment on a lot of the same topics, and assumptions, and speculations as are here, and the judge found that there was insufficient evidence to preserve even an issue for trial.

As a matter, he dismissed --

THE COURT: Was there a standing dispute in that case?

ATTORNEY PATTON: Yes, there was, your Honor. It was a standing dispute.

THE COURT: So, it must have gone beyond standing.

ATTORNEY PATTON: The standing and the merits were dealt with at the summary judgment stage. It was a motion for summary judgment -- partial motion for summary judgment by the Jewel plaintiffs on their Fourth Amendment claim. And the United States, Connor, cross-moved for summary judgment on that.

THE COURT: And who were the plaintiffs in that case.

ATTORNEY PATTON: The plaintiffs or Jewel was one plaintiff and another particular plaintiff --

THE COURT: So, these parties were not parties.

ATTORNEY PATTON: These plaintiff were parties to the case; that's correct.

THE COURT: They were.

ATTORNEY PATTON: Yes. So, they, basically, and much the same way as the plaintiffs in this case said, there has been so much information out there in the public sphere since the Snowden --

THE COURT: Well, we will get to argument about standing. I just want to focus now, very sharply, on -- I have asked you the question, are there any other cases that are recent or ongoing, involving a challenge to the NSA's collection upstream of this Internet data.

And you've told me about one in California that went to summary judgment. Was there a Ninth Circuit appeal?

ATTORNEY PATTEN: So, there is a Ninth Circuit appeal currently ongoing on that issue, your Honor. But there is also a motion to dismiss the appeal that is being heard later in October, because it was a Rule 54(b).

THE COURT: All right.

And the plaintiffs here were plaintiffs there as well.

ATTORNEY PATTON: No, that's not correct, your Honor. None of the plaintiff there, to my knowledge, were plaintiffs.

THE COURT: Am sorry. I thought you said earlier, they were.

ATTORNEY PATTON: No. They are making the same arguments.

THE COURT: Oh, making the same arguments.

ATTORNEY PATTON: Making the same arguments.

THE COURT: All right.

ATTORNEY PATTON: The plaintiffs here.

THE COURT: All right.

Apart from the California case, any other?

ATTORNEY PATTON: I am not aware of any others on the civil side. Obviously, on the criminal side, there is a Hasbarjrami case that, I think, the ACLU filed an amicus brief on that, in that particular case, challenging both upstream and PRISM.

So, but, as far as civil cases are concerned, I am not aware of any other upstream challenge other than this one and the one in the Northern District of California.

THE COURT: All right.

ATTORNEY PATTON: And there are other civil actions under Section 702, but those are all PRISM cases challenging a different program.

THE COURT: All right.

Now, the second question I want to ask you is -- well, no, I'll make it the third, because the second question I am going to ask you is probably going to take longer.

So, I'll ask another question first. I take it that at some point in time, or points in time, the data collection that the NSA is undertaking that is being challenged in this case went to the FISC -- went to the Foreign Intelligence Surveillance Court, and an order issued.

ATTORNEY PATTON: That's correct, your Honor. The process works under Section 702.

THE COURT: Right.

ATTORNEY PATTON: The Attorney General and the --

THE COURT: But there is, usually, an order and an opinion sometimes with it. Did that occur? And the reason I know that is that I have had a number of classified information cases here. We get cases of that sort here, and I have had to consider those orders and those opinions.

Most of them have been -- most of them, there only have been two or three -- have been classified.

Is there a public order or opinion in -- that relates to the data collection practices challenged here?

ATTORNEY PATTON: I don't believe there is an unclassified opinion.

THE COURT: But there would have to be a classified order and/or opinion; is that right?

ATTORNEY PATTON: Certainly a classified order because --

THE COURT: All right.

ATTORNEY PATTON: -- FISC has to approve both the certification coming from the Attorney General and the Director of National Intelligence --

THE COURT: So --

ATTORNEY PATTON: -- plus their targeting procedures and minimization procedures.

THE COURT: So, let me continue for just a moment and ask you, what, if any effect, should the existence of such an order have on the challenge by the plaintiffs in this case?

ATTORNEY PATTON: For purposes of them being able to prove their standing, I don't believe it has any. For purposes of, if this case goes to the merits, I think it has a significant impact on it because -

THE COURT: All right.

ATTORNEY PATTON: -- the FISC has to prove the reasonableness of the program under the Fourth Amendment that's under the statute. And both the --

THE COURT: So, it would be akin to something like the existence of a search warrant in a case challenging the legality of the search.

The court would still have to assess whether the search was legal, and defects in the search warrant, or the affidavits, or whatever, would have to be examined.

All right. Let's go to the third question, which really leads into what's at issue today. The first two questions I asked really don't have much to do with what's before the court today.

The Clapper case is a case that you rely on quite significantly. Now, what -- and that was upstream collection data, was it not?

ATTORNEY PATTON: That was Section 702, which authorizes upstream selection and authorizes PRISM. But it was a facial challenge brought, in fact, by six of the nine plaintiffs here, a facial challenge to the statute that authorizes this very program.

THE COURT: Now, what -- and, of course, Clapper held there was no standing in a divided court.

ATTORNEY PATTON: Well, divided in the sense that it was five, four. But, yes, the majority ruled that there were no standing for the same reason --

THE COURT: Yes.

ATTORNEY PATTON: -- were pending in this case.

THE COURT: Now, I want to know -- and I am going to ask this of the -- of you, Mr. Toomey.

What is there in this second or amended complaint that is different from or in addition to the facts that were alleged in Clapper?

And I ask that for an obvious reason. And that is, that if the facts in this case are exactly the same as Clapper, no different from Clapper, then I don't know that I have the authority to reach any different conclusion.

So, I want to know whether, chiefly from you, Mr. Toomey, what is alleged in this case that is different from or in addition to what was alleged in Clapper.

ATTORNEY PATTON: Your Honor, if I may answer that question as quickly as I possible, because there are, obviously, a lot of things that are alleged.

But the bottom line here is that in Clapper the Supreme Court ruled that the plaintiffs in that case could only speculate and make assumptions about who the targets were.

Here the same kind of speculations and assumptions have to albeit, by these plaintiffs, as to whether or not their communications were intercepted. So, it's only sightly different, but it's the speculation on the assumptions that's key.

And here, whether -- whether anyone that these plaintiffs are talking to is a target, classified. Whether, what the scope of upstream collection is, how it actually operates, classified.

So, the only things that the plaintiffs can do, as set aside and throw against the wall, as much information as they can taken from this snippet or that snippet, but the bottom line is, they have to say, you must be collecting this. It's speculation. You've got to do it in this way in order to be effective.

And the D.C. Circuit through Judge Sentelle and Judge Williams, just last month, looked at albeit the bulk telephony metadata program in that case, and said that's not enough.

When you are looking at a program and

saying, well, in order to be effective as a bulb telephony metadata, you must be collecting from Verizon wireless. That's just one piece of speculation. And I know that we are going to hear from the plaintiff about a chain of speculation in Amnesty and that there is not as long a chain here. The point is, it's still speculation.

And one case of speculation was sufficient for the D.C. Circuit to say, you've not shown standing in that case. That was one of the cases that your Honor alluded to earlier.

And the point is, the plaintiff in that case could not say, following Amnesty, that just because we think the program would be effective, only if you had Verizon wireless, that we can presume that Verizon is part of the program.

Here, plaintiffs make the same arguments. We presume it has to be substantially all because, otherwise, how could you do this, or how could you do that?

And, of course, the point is how the program operates is classified. There are very few pieces of information out there in the public. There is Privacy and Civil Liberties Oversight Board. There are some FISC opinions. I recommend 2011 FISC opinion from

October 3rd of that year by Judge Bates, which explains a lot about this program. But what it doesn't explain is the scope of the program, the operational details of how it works. Those were classified, and they are still classified.

So, plaintiffs, they will tell you a lot of things together, and their words would be, they must be doing this. To be effective, they must do this. Those are all speculative words. They are all assumptions that the plaintiff make.

So, notwithstanding the pieces of information that have come out, official acknowledgement since the Snowden leaks that occurred, nothing that has come out as an official acknowledgement has indicated in anyway the scope of this program or how it works.

The plaintiff are left to speculate. That's exactly what the Supreme Court said they can't do in order to show standing on page 1148 of the Clapper versus Amnesty opinion.

So, we submit this case is not that difficult, notwithstanding the forest that we killed to prove the point to you, is that plaintiffs, two years later, cannot get any further than the -- six of the same plaintiffs did in Clapper versus Amnesty International.

THE COURT: I take it you would not contest standing if the plaintiffs adduced an e-mail of theirs that they got from Snowden saying he got it from NSA.

ATTORNEY PATTON: That would be very fact specific, your Honor. Obviously --

THE COURT: And then it would be the credibility of Snowden.

ATTORNEY TOOMEY: Well, I am certainly not going to address that. But what I will address is official acknowledgments, for example --

THE COURT: Well, I think, what my question really was is how in the world does the plaintiff in this situation show standing other than by inference and probabilities?

ATTORNEY PATTON: Well, your Honor, that certainly a problem that the plaintiffs at Amnesty International had. And, as I alluded earlier, the ACLU on behalf of Mr. Hasbarjrami, he received an official notice, not specific to upstream collection or PRISM, but a 702 notice that the parties have discussed in their papers. And so they briefed that issue of the legality of Section 702 upstream and PRISM, and so those issues were briefed.

If some plaintiff came forward with evidence that they had, in fact, being -- their communications being intercepted, then certainly we would look at that and the facts of that case.

THE COURT: How in the world would they get that evidence?

ATTORNEY PATTON: Well, that's -- that's one of the features of a classified program. It's not a bug of a classified program that it's hard to prove standing.

THE COURT: Yes. And you couldn't and shouldn't tell me how they could get that because you would be revealing, if you knew --

ATTORNEY PATTON: Right.

THE COURT: -- classified information.

ATTORNEY PATTON: That's correct.

THE COURT: I am just making the observation that, I am sure, was apparent to the Supreme Court in Clapper that this is a significant, very difficult burden for a plaintiff that they are setting.

And in one of -- life is full of ironies. I believe Justice Breyer was an author of either Iqbal or Twombly. I don't remember which one.

Which one was anti-trust case?

ATTORNEY PATTON: I think they were both anti-trust case.

THE COURT: Well, one of the --

ATTORNEY PATTON: Twombly, I am sorry. Twombly was anti-trust case.

THE COURT: I think Breyer authored Twombly; and, of course, he doesn't -- he is not happy with its application, as the majority put it in this case. Just an irony that I -- I am increasingly amused by in life. There are lots of them in everyone's lives.

I think I understand the parties' arguments. Let's do this. You'll have the last word. You are the movant. But let me ask Mr. Toomey to tell me. And pay attention to this because this is one of the things that I do want you to respond to.

My first question to Mr. Toomey is the obvious one. What has been alleged in this case that is different from or in addition to what was found to be insufficient in Clapper?

ATTORNEY TOOMEY: Of course, your Honor.

There are four reasons.

THE COURT: I am sure that's a question you anticipated.

ATTORNEY TOOMEY: We had an idea you might ask it, your Honor.

THE COURT: All right.

ATTORNEY TOOMEY: There are four basic reasons this case is not foreclosed by Amnesty

International, your Honor.

And if I can just describe in each briefly and then get into more detail, if you you want to go further. The first reason is that this surveillance is fundamentally different from the surveillance that was at issue in Clapper.

The surveillance at issue in Clapper concerns what the Supreme Court understood to be targeted surveillance, surveillance that was directed at the communications to or from the government's foreign targets.

The surveillance that has been disclosed now, and officially acknowledged by the government, is far broader than that. It involves, in the first instance, this screening, as the government calls it, and as we refer to it, the copying and reviewing of, essentially, everyone's communications, targets and non-targets alike, in search of certain terms that are associated with the government's targets.

So, to put it maybe more simply, your Honor, to put in terms of physical mail, for instance. If the government wanted to collect mail from its -- from just its targets, it could look at the outside of the envelope and say, I'll take this letter and that letter.

If the government wanted to find the letters containing the e-mail address or the name of a target, it would have to look at the content of every letter coming through, you know, the postal screening service in order to find the communications that it was looking for.

And that's very important to know about what this surveillance entails. And it was not before the Supreme Court in Clapper, precisely, because, as others have observed since, the government did not inform the Supreme Court that that was how some of the surveillance was being conducted.

The second difference, your Honor, is that far, far more is known -- is now known about the surveillance than was known at the time of Clapper.

And the PCLOB report makes this point explicitly. And we, we identified that statement in paragraph 51 of our amended complaint, that at the time Clapper was decided and, in fact, when the statute was passed, no one in the public or the Supreme Court understood the surveillance to operate in this way; that is, to be this broad net looking at the content of all the transiting communications, as opposed to merely being focused on the communications of targets.

And we have pointed to numerous other official disclosed -- disclosed documents that showed this. We don't have the FISC order in the terms that, perhaps, you were asking before that authorizes this surveillance.

But we certainly have FISC opinions that you can find on Westlaw, in fact, that describe the surveillance at issue, that describe upstream surveillance. And one of those opinions is an opinion from Judge Bates from October 2011, where he found certain of the procedures that govern upstream surveillance unconstitutional.

And there are other opinions out there that are also touching surveillance that have been released by the government. So, the record that the court has before if today about how this surveillance operates, the government says everything about how this surveillance operates is classified. Well, that's not true.

The PCLOB report describes in a number of ways how this surveillance operates.

THE COURT: What report?

ATTORNEY TOOMEY: The PCLOB report, your Honor. That's the Privacy and Civil Liberties Oversight Board report. It's a 196-page report that evaluates the government's surveillance activities under Section 702.

It describes upstream surveillance in

significant detail, and many of the key points are identified, both in our briefs, and in our amended complaint.

The third difference from Amnesty is that the plaintiff are different, not merely in their name, your Honor, but in terms of how they communicate and the volume and distribution of their communications.

We have pointed, specifically, to Wikimedia's communications. It engages in more than trillion Internet communications, international Internet communications each year with individuals in every country on earth.

No -- none of the plaintiffs in Amnesty put that record before the court. And we've also put before the court a member of NACDL, Mr. Dratel, whose clients received an FAA notice. In other words, whose client was told that the government used FAA surveillance to intercept --

THE COURT: Say that last again, please.

ATTORNEY TOOMEY: Say which part again, the last part?

ATTORNEY TOOMEY: Mr. Dratel's client received a notice from the government, an official notice, that his communications were intercepted using FAA surveillance.

And Mr. Dratel had a second client whose investigation involves a co-defendant, who also government officials have described in testimony using FAA surveillance.

THE COURT: That just shows that those particular communications were gathered. And for all we know, those persons' clients were designated terrorists overseas, right?

ATTORNEY TOOMEY: The lawyers' clients were individuals here in the U.S.

THE COURT: But were they -- certainly, if they were people they were communicating with were terrorists, that wouldn't be a problem, Constitutionally, would it, if they were communicating overseas and there was a FISC court order that permitted it.

ATTORNEY TOOMEY: Our argument here, your Honor, is that the facts that --

THE COURT: Can you say yes or no and then answer my question, and then go to explain it. It's frustrating when I ask a question, and I -- this isn't politics. This isn't -- you are not on the stump. It's better to give me a direct answer.

If the person who received these notices was communicating, or not the person receiving notice, but the client was communicating with someone who was a designated terrorist or something of that sort overseas, then nothing constitutional -- unconstitutional about that if there is a FISC order, is there?

ATTORNEY TOOMEY: We think there is something unconstitutional with that, your Honor. That's not the issue here right now.

To be very clear about the type of FISC orders that are involved in Section 702 surveillance, they are not individualized warrants or individualized orders finding probable cause of the same kind, as what we refer to as a traditional FISC order.

They are the FISC orders that apply to this surveillance part, general orders authorizing and approving the procedures that the government proposes to follow.

The government never identifies through the court its particular targets. And, in fact, those targets do not need to be designated terrorists at all. They could -- they can be any foreigner located abroad, any person who the government believes has -- is likely to communicate information with foreign intelligence value to it. It could be journalists. It could be human rights activists. It could be academics. It could be individuals who work at companies abroad.

So, I just want to be very careful to distinguish between what -- what the traditional FISC process required, which was and had done an individualized order, and the surveillance at issue here in which the government is able to identify 92,000 targets, foreign targets, under a single FISC order.

And we do believe that there are grave constitutional problems with the government's ability to do that absent some type of probable cause finding required by the Fourth Amendment.

Back to Mr. Dratel, your Honor, because -- and the lawyer who has a client who received one of these notices. Our argument is -- and the Supreme Court made this point in Amnesty itself, the five justices in the majority.

The court observed that an attorney whose client was subject to FAA's surveillance would be able to make a stronger evidentiary showing that his communications had been intercepted, than the plaintiffs who are before the court in Amnesty.

And the reason that we believe we have made that this type of stronger showing here is because in order to investigate a defense, in order to contact witnesses abroad, when a defendant has received a notice, the defendant's lawyer must reach out to individuals abroad, contact key witnesses, research the allegations in the indictment, and that that lawyer is likely to communicate with or about the same person who was targeted through the FAA surveillance.

So, that's why we believe the facts that Mr. Dratel puts before court are very different from the lawyers who were before the court in Amnesty itself.

But the third point is more generally that Wikimedia's communications are so widely distributed across the globe and so immense in number that they transit all of the major Internet circuits that the government is monitoring.

So, whichever circuits the government is monitoring, our arguments is, the government must be intercepting at least some of plaintiffs' Wikimedia's communications.

The fourth point, your Honor, is that the legal standard in this case is different from the legal standards in amnesty. We are here, of course, on a motion to dismiss. The government says the legal standard is plausibility.

In Amnesty, the parties were before the court on a motion for summary judgment. And the Supreme Court has emphasized in a number of different places and a number of different ways that what a party is required to put forward at the pleading stage is different than what a party must put forward at the summary judgment stage.

So, those are the main four categories in which we think this case is very different from Amnesty. You can also see this in concrete way by comparing the facts of this case to contingencies that Justice Alito identified on page 1148 of the court's opinion.

First he said -- you know, he said that the court was considering a set of contingencies that the plaintiff was putting forward. The first of them was that the government would target the plaintiffs' contacts.

Now, the surveillance -- because the surveillance here is different, because it involves examining the content of, essentially, everyone's targets and non-targets communications, the fact that the surveillance implicates plaintiff doesn't depend on whether the government is surveilling plaintiff's individual context.

Second, the second contingencies that Justice Alito identified was that government would choose to use FAA surveillance.

But, of course, the government has officially disclosed that it is using upstream surveillance; and the PCLOB, the Privacy and Civil Liberties Oversight Board, has described that surveillance, and it has been described in another number of other context by the government.

Third, justice Alito said that the plaintiffs in that case could not know whether the FISC had approved the surveillance. But, of course, here we know that for a fact that the FISC had approved the surveillance.

The government just told you that and, of course, it is reflected in the materials that we cited in the paper and in the amended complaint.

And, fourth, the Court said that plaintiffs were speculating about whether the surveillance would implicate their communications.

But we have put forward facts showing that this surveillance implicates the plaintiffs' communications. We have alleged first that the government is intercepting, it's copying, and reviewing substantially all international communications, including those of plaintiffs; and second, even if that were not enough, we have alleged facts showing that the government is copying and reviewing at least some of the plaintiffs' trillion or more communications each year.

And that showing, I want to emphasize, we are saying to a virtual certainty that the government, in order to carry out upstream surveillance, must be copying and reviewing at least some of the plaintiffs' communications.

We say that based on three factual premises, your Honor. First, the facts that the government, itself, has acknowledged about how upstream surveillance operates.

The PCLOB has described -- the Privacy and Civil Liberties Board has described in analyzing precisely this type of surveillance, the use of surveillance devices that examine the content of all communications transiting that device.

And it has put forward even more detailed description about how the government's review of the contents of communications requires it to access, not just the communications of targets, but the communications of others.

Second, we have appointed to the volume and distribution of plaintiff Wikimedia's communications. The fact that Wikimedia's communications are so numerous and spread across the globe that they transit every major Internet circuit entering and leaving the country.

And third, we have pointed to technological requirements of -- for conducting this type of surveillance. And we have explained those technological requirements and the structure of Internet communications in great detail in our papers.

And those -- those technological requirements are consistent with the analysis of computer experts that are cited in the New York Times article that we also rely upon which says, based on interviews with government officials, review of NSA documents, and conversations and -- conversations with computer scientists that in order to carry out this type of surveillance the government would have to be copying and reassembling, essentially, all the tiny packets that are flowing in the stream of data in order to review and identify the communications of its 92,000 individual targets that are spread across the globe.

And we believe we can make this showing, your Honor, on the basis of information that's in the public record. But, of course, we have also pointed the court to materials that corroborate plaintiffs' showing on these points that show that the government is conducting the surveillance at many choke points and that it has identified and pointed to plaintiff, Wikimedia's, own communications in connection with upstream surveillance.

THE COURT: All right.

Thank you.

ATTORNEY TOOMEY: Do you have any further questions, your Honor?

THE COURT: No, thank you.

You will have the last word. But I want you to respond, specifically, to what Mr. Toomey has said. He went through -- he counted four. I counted five differences between -- that he contends exist between this and the information available in Clapper.

ATTORNEY PATTON: Yes, your Honor. I am happy to walk through them all. The first one that I wrote down was that the -- what we have here, upstream collection, is "fundamentally different" than Section 702 that was at issue in Clapper.

First of all Clapper versus Amnesty International involved 702. 702 has upstream and PRISM. What wasn't public at the time was that upstream collection includes to, from, and about with regard to Internet communications.

What does "about" mean? The plaintiffs used this phrase as if talking about Rodney Patton was a target, that if they sent an e-mail with Rodney Patton in it, that that will show up and that's something that would be captured. That's not correct.

"About" relates to the specific

communications identifier, such as an e-mail address. So, in the context of an about communications, so the about could appear in the header or appear in the body.

If you want to know more about making a bomb, contact following e-mail. That is an about communication.

The most critical point, I think, that the plaintiffs make in their first point is, and they keep repeating it throughout is that we are copying, essentially, everyone's communications, essentially everyone's international communications.

That's not well pled under Iqbal at all. That's their conclusion. Any factual enhancement that they have suggested to support that, doesn't.

Mr. Toomey refers to the PCLOB report, for example, and there are plenty of facts about the upstream collection in this program.

What there isn't is any discussion about its scope and operational details. I want to give you one example that they cite to demonstrate that is, essentially, everyone's communications. That's page 111, note 476.

"The NSA's upstream collection may require access to a larger body of international communications than those that contained a tasked selector." May require access to a larger body. How big, how small is that? PCLOB doesn't say, nor does the FISC opinion that both the plaintiffs and the defendants have cited and referenced to you today.

And that the FISC opinion talks about nine percent of the 702 collection being related to upstream and 91 percent being related to PRISM. That was in 2011.

That doesn't tell you anything about the extent and scope of whether, essentially, everyone's communications were copied. The same is true on the ODNI report.

The Office of Director of National Intelligence report, where it referenced there are over 92,000 targets for 702. How many are PRISM? How many are upstream? You are left to guess.

There is the Charlie Savage article from the New York Times in 2013. Again, media speculation about the extent. There is no actual knowledge in there.

In fact, the PCLOB report references this particular article on page 119 and with reference to about collection, says that that article misunderstands the more complex reality.

And that's the problem with speculation, of course, is that you don't understand what is, actually, going on. There is reference to their technical capacity. Of course, under Iqbal, if you have the technical capacity to do something, that doesn't mean you are doing it. It is, consistency, as Iqbal pointed and Twombly pointed out, is not enough.

There are a limited number of choke points they indicated. 49, I think, is the number they used. But that number doesn't mean one thing or another with regard to how much of that the NSA is monitoring.

The purported slide that is on paragraph 68, I think, of their complaint, we can neither confirm nor deny its authenticity. But even if it's correct doesn't support the proposition that they want this court to draw from it.

It indicates or purports to indicate that there is coverage on some, but that doesn't mean all. So, the bottom line there is, with regard to it being fundamentally different, it is not.

And then far -- their second point, which I have, obviously, touched on here, is that far more is known about it. I have walked through the PCLOB report and FISC opinion. And this I could talk a lot about, this next point, but I will spare you all of the details.

The plaintiffs are different. Well, eight out of the nine plaintiffs are not different. Eight out of the nine plaintiffs are pretty much the same as the plaintiffs in Clapper versus Amnesty International.

The one that is different here, they say is, Wikimedia. Why? They have a huge volume of communications, they said, distributed throughout the world.

These communications, of course, are someone like -- someone from France logging on and looking up a Wikimedia website. That's a communication here. They have over a trillion of those, they say.

Well --

THE COURT: Their counting of the trillion is subject to some dispute.

ATTORNEY PATTON: It is subject to some dispute.

THE COURT: Put it to one side, because it is a large number, they are counting every little bit.

ATTORNEY PATTON: Well, what they are counting are http requests. And, as our expert pointed out, http request for a Wikimedia article is a lot fewer than, say, if you are going on FISC, both because http requests would get more, the more complicated the graphics and the adds, and there are no adds on Wiki cites, and there are not as many graphics.

So, even that one trillion number is comparing apples to oranges in terms of the website visits that we've looked at and the web page views.

So, if you look at Wiki's web page views, though, and you compare just that for all the Wiki cites that they have -- I think it was 255 billion per year, it actually amounts to, when you combine just the e-mails that traverse the world, and the top 50 websites -- top 50 out of 244 million active websites out there. It's still 0.29 percent.

So, the terms of volume, the numbers seem staggering until you put it in context. They didn't put it in context, and we have done that here.

Plaintiffs talked about Mr. Dratel and Mr. Dratel's clients. Mr. Dratel's clients received a notice of Section 702 surveillance, that their case involved that.

What they didn't get was, is it an upstream case. So, he has to speculate, well, was it an upstream surveillance? Was it a PRISM surveillance? They are not told.

So, what they do in those criminal cases is they brief the legality of both. But that's fine for them to do in a criminal case. But here they need to show something more than just a mere possibility --

could have been that, could have been this. You decide. That's the mere possibility under Iqbal standards.

Again, when talking about this, he -- the plaintiffs indicated that there is a virtual certainty that we must be intercepting, and those are those speculative words.

Once you are here you, must be doing something. They must be doing this to make it effective. That's the words of speculation from page 1140 of the Clapper versus Amnesty International that says, "Assumptions and speculations are not enough."

Mr. Toomey mentioned the legal standard, and we are here on the motion to dismiss. We are here on an motion to dismiss. But we are here on an unusual sort of framework because some of the allegations have been attacked under the plausibility standard under Iqbal like the substantially all. There is no plausible allegation in there supporting that.

But they are also -- the government has attacked the factual underpinning of many of their allegations, including the key one that is a virtual certainty that volume, for example, demonstrates that Wikimedia has standing or that if you are on one cable you must be collecting all of that. That's not true as a matter of technology, and our expert pointed that out.

So, even if we are on one cable, that doesn't mean that all communications on that cable are subject to interception. That's the takeaway.

But those kinds of factual disputes put the factual burden on the plaintiffs to show, by a preponderance of the evidence, and your Honor can see that in United States ex rel. Vuyyuru versus Jadhav. And I probably have the cite here, 555 F.3d 337 at page 337. That's a Fourth Circuit case from 2009.

So, from the perspective of the legal standard, yes, there is a little difference because it was up on summary judgment at that time in front of Clapper. But up on summary judgment, the court find there wasn't even a genuine issue of material fact to take beyond summary judgment from Clapper.

In fact, there are cases that this argument started out talking about Jewel versus NSA in the Northern District of California. Same result.

This is the Clapper case versus Amnesty International both 702, this case and the Jewel case involved 702, but upstream collection specifically.

THE COURT: Clapper went on summary judgment. I take it in -- at the dismissal stage in Clapper, there was an objection to the plaintiff's standing.

ATTORNEY PATTON: I believe -- I believe it went to -- Mr. Capilano, who was here earlier was -- handled that case on behalf of United States.

THE COURT: I'm sorry. Say that again, please, sir.

ATTORNEY PATTON: I am afraid I was not on that case. I believe Mr. Jaffer was from ACLU. But my recollection of the procedural posture was that that case went directly to merits briefing. That's correct. And so it was summary judgment brief. And there was no opportunity, like there is here, for your Honor to dismiss this case without going forward to the merits and whatever could happen at the merits stage.

THE COURT: All right.

Thank you.

ATTORNEY PATTON: Thank you. I have much more I could say, but there is a lot of information in the briefs.

THE COURT: You don't get the last word. You are not the movant.

ATTORNEY TOOMEY: I understand, your Honor. I had hoped that we could say something about the procedural posture of the case.

THE COURT: All right. Go ahead. And then I'll give you the last word, because you are the movant;

and, otherwise, it's interminable, and it's lunch time.

ATTORNEY TOOMEY: I understand, your Honor. The government just explained that it now views its case as both a facial attack on the complaint and a factual attack on the complaint.

And I want to explain and make very clear, I hope, to the court why the government is trying to have it both ways, and why that's inappropriate at this stage of the case.

The government is trying to have the benefit to prevail on a motion to dismiss, using evidence that it's only entitled to the merits. And there are three reasons, if I can describe those for the court.

The first is that Fourth Circuit has made very clear, including in a case the government just cited to you that when the factual issue in dispute is inextricably intertwined with the merits, it can only be resolved on the merits under Rule 56. And that's not what the government is proposing to do here.

The fact of whether the government is copying and reviewing the plaintiffs' communications, obviously, is closely related, if not an essential element of plaintiffs showing that the government is unlawfully searching and seizing their communications.

It would be like a plaintiff suing over an illegal house search, and the government saying, as a jurisdictional matter, we want you to prove that your house was searched and how it violated your privacy under Rule 12(b)(1).

And the Fourth Circuit's decisions in Kearns, in United States versus North Carolina, in Vuyyuru, which is a case the government just cited, and in Adams, all show to the contrary, that this factual dispute can only be resolved on the merits.

The second point is that the government didn't present --

THE COURT: It isn't a factual dispute. It's a dispute about whether the allegations in the complaint, the amended complaint, are sufficient to raise a plausible inference that your clients' communications were seized and copied. That's what is it at the threshold.

ATTORNEY TOOMEY: We entirely agree with that, your Honor. And our --

THE COURT: If we get into the facts and -- I think I -- you may be seated.

Let me ask the government. You don't intend to make it a factual determination, do you?

ATTORNEY TOOMEY: There is a portion of the motion to dismiss that we filed, and Mr. Toomey mentioned that I just explained.

We explained this situation, what was happening in our reply brief, as to what -- because they not moved to strike, but indicated that it was improper for us to add documents outside the pleadings, the two expert declarations, for example.

But for the substantially all-allegation, that is, clearly, unsupported by any well-pled allegations in the complaint. As your Honor mentioned, it's an Iqbal plausibility determination.

When we get to the part of, they must -- the NSA must be conducting surveillances, obviously, it's speculation the say way as it was in Clapper versus Amnesty.

But if your Honor needs to get to any factual issue on that, you can also resolve that short of a merits determination to decide jurisdictional facts.

And I have heard the plaintiffs say, both in their brief and here today, that the facts are inextricably intertwined. But I have not heard how it is. In every case you have to show standing, and in every case --

THE COURT: Standing is a jurisdictional --

ATTORNEY PATTON: It's a jurisdictional

matter.

THE COURT: Just a moment. When I start, you need to stop.

ATTORNEY PATTON: Sorry.

THE COURT: He gets us only one at a time here, Mr. Rodriquez.

ATTORNEY PATTON: Too much coffee this morning.

THE COURT: And it's a jurisdictional issue. I have no power to decide the merits until I decide the jurisdictional issue.

Only if I find standing, do I have the power to adjudicate. I am not a fan of mixing standing with the merits, and going ahead.

I am surprised that the California suit, once you get past the jurisdictional aspect then, of course, you get discovery. I would be surprised if everybody doesn't have to get some kind of clearance to look what discovery is sought.

And, so, I don't see this as a case involving a factual dispute, do you?

ATTORNEY PATTON: I don't believe so.

THE COURT: This standing issue, I don't have to resolve a factual dispute, do I?

ATTORNEY PATTON: As the record exists right now, your Honor, I don't see -- I think we can resolve this case on --

THE COURT: So, I don't have to look at your declarations.

ATTORNEY PATTON: If you can decide this without the declarations, we are certainly --

THE COURT: Well, if I have to use the declarations to decide them, isn't that importing into the standing?

Let me do this. Mr. Johnson, I am going to take a recess before I hear your case, so that we can have lunch.

ATTORNEY JOHNSON: Yes, sir.

THE COURT: So we wouldn't begin your case until 1:30 at the earliest.

ATTORNEY JOHNSON: Yes, sir.

THE COURT: Now, your client, I think, is in the custody of the marshals. If you need to see him, you need to discuss that with the court security officer and the marshals.

ATTORNEY JOHNSON: Yes, sir, I will. That is what I am trying to do. I appreciate that, your Honor.

THE COURT: Thank you, Mr. Johnson.

All right. So, I want to be clear, do you

you believe -- is it the government's position that I have to resolve factual disputes, other than inferences. You are going to disagree about inferences.

But, do I have to get into the merits, facts of this, that is seizing of actual things to decide the case -- decide the standing issues.

ATTORNEY PATTON: You do not need to -- that's our point is that, contrary to what the plaintiff say, you do not need to get into the merits FISC facts because the merit FISC facts are not inextricably intertwined.

To the extent that at the end of all the briefing you think that there are any jurisdictional factual disputes, you are entitled, as a matter of law, in determining your jurisdiction, to resolve those.

THE COURT: All right. A last question for you. Other than producing an e-mail of the plaintiffs that they can show was trapped, and copied, and whatever by the NSA, is there any other way to get standing?

ATTORNEY PATTON: Certainly, if there is an official acknowledgement by the United States in a criminal case, if they said, we took this information from you, from the upstream process, then I can envision that.

THE COURT: But, in this context, you can't think of any?

ATTORNEY PATTON: I can't think of any --

THE COURT: Other than what the --

ATTORNEY PATTON: -- right here, but I will say that the Supreme Court -- this same argument was made to the Supreme Court. And the response to the Supreme Court was, just because you don't have standing, and you can't think of anybody who does, there is no reason to find standing in this case.

THE COURT: Yes, I think that's clear. But no judge could decide this without thinking about that. And you would not, I think, argument on behalf of the government that just because you all keep things secret that the constitutionality of it can't be, at some point, examined and judicially determined.

ATTORNEY PATTON: Well, two points, your Honor. The constitutionality of this program is, at least, once a year examined by the Foreign Intelligence Surveillance Court that has --

THE COURT: That's the question I asked. That's the point I raised at the outset. Where are the opinions and the -- from the FISC court? And the answer to that was, well, they only decide the minimization efforts and so forth.

ATTORNEY PATTON: They decide -- they have to decide whether the process that's in place, the minimization procedures and targeting procedures, are reasonably designed to comply both with the statute, Section 702, and with the Fourth Amendment, with full knowledge of how, from the NSA and from the National Security Division, Department of Justice, how this program works, not something that we --

THE COURT: The only thing missing from that equation is anybody arguing that it's unconstitutional.

ATTORNEY PATTON: Well, your Honor, as you know, the USA Freedom Act was enacted just a few months ago, and there are issues that are coming from that about designing particular parties to argue those --

THE COURT: Yes.

ATTORNEY PATTON: -- those kinds of --

THE COURT: Yes.

ATTORNEY PATTON: -- those kinds of things.

But the second point is, who can make these arguments. In criminal case, the ACLU is making these very arguments and has made them on behalf of Mr. Dratel's clients that -- that upstream collection is unconstitutional, that it violates the Fourth Amendment at the very least.

So, whether these particular plaintiffs are able to demonstrate to the court's satisfaction they have standing or not, these issues are being addressed by article three judges.

THE COURT: Thank you.

ATTORNEY PATTON: Thank you, your Honor.

THE COURT: Obviously, this is an issue of some complexity and importance. I think the arguments today have been helpful, and I thank counsel for that.

The purpose of oral argument is two-fold. One is to focus matters sharply, and I think this has focused it reasonably sharply on issues. And the other is to expose my ignorance so you could fill the empty bottle, as it were, and you all have done that in your briefs and now in oral argument, and I thank you.

Again, I thank counsel for your cooperation, particularly, for your agreement to have your argument here rather than at Greenbelt.

Court stands in recess.

(Court recessed at 1:03 p.m.)

CERTIFICATE OF REPORTER

I, MICHAEL A. RODRIQUEZ, an Official Court Reporter for the United States District Court, in the Eastern District of Virginia, Alexandria Division, do hereby certify that I reported by machine shorthand, in my official capacity, the proceedings had and evidence adduced upon the motion hearing in the case of WIKIMEDIA FOUNDATION, et al vs. NSA/CSS.

I further certify that I was authorized and did report by stenotype the proceedings and evidence in said motion hearing, and that the foregoing pages, numbered 1 to 52, inclusive, constitute the official transcript of said proceedings as taken from my machine shorthand notes.

IN WITNESS WHEREOF, I have hereto subscribed my name this 1st day of October, 2015.

/S/

Michael A. Rodriquez, RPR/CM/RMR
Official Court Reporter

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION, *et al.*,	)	
Plaintiffs,	)	
	)	
v.	)	**Case No. 1:15-cv-662**
	)	
NATIONAL SECURITY AGENCY /	)	
CENTRAL SECURITY SERVICE, *et al.*,	)	
Defendants.	)	

MEMORANDUM OPINION

This is the latest in the recent series of constitutional challenges to the National Security Agency's ("NSA") data gathering efforts.[1] In this case, plaintiffs, nine organizations that communicate over the Internet, allege that the NSA's interception, collection, review, and storing of plaintiffs' Internet communications violates plaintiffs' rights under the First and Fourth Amendments and exceeds the NSA's authority under the Foreign Intelligence Surveillance Act ("FISA"). Typical of these challenges to the NSA's surveillance programs is defendants' threshold jurisdictional contention that plaintiffs lack Article III standing to assert their claims. This memorandum opinion addresses the standing issue.

---

[1] *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013) (involving a facial challenge to Section 702 of the Foreign Intelligence Surveillance Act); *Obama v. Klayman*, Nos. 14-5004, 14-5005, 14-5016, 14-5017, 2015 WL 5058403 (D.C. Cir. Aug. 28, 2015) (involving a challenge to the NSA's bulk collection of telephone metadata produced by telephone companies); *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (involving a challenge to the NSA's bulk telephone metadata collection program); *Jewel v. Nat'l Sec. Agency*, No. C 08-04373, 2015 WL 545925 (N.D. Cal. Feb. 10, 2015), *appeal docketed*, No. 15-16133 (9th Cir. June 4, 2015) (involving a challenge to the NSA's interception of Internet communications).

I.[2]

The nine plaintiff organizations are as follows:

- Wikimedia Foundation ("Wikimedia") is a non-profit organization based in San Francisco, California, that maintains twelve Internet projects—including Wikipedia—that provide free content to users around the world.

- The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C., that focuses on criminal defense matters.

- Amnesty International USA, headquartered in New York City, is the largest division of Amnesty International, which focuses on human rights around the world.

- Human Rights Watch is a non-profit human rights organization based in New York City.

- PEN American Center is an association based in New York City that advocates on behalf of writers.

- Global Fund for Women is a non-profit grant-making foundation based in San Francisco, California, and New York City, that focuses on women's rights around the world.

- The Nation Magazine, published by The Nation Company, LLC, is based in New York City and reports on issues related to international affairs.

- The Rutherford Institute is a civil liberties organization based in Charlottesville, Virginia.

- The Washington Office on Latin America is a non-profit organization based in Washington, D.C., that focuses on social justice in the Americas.

The six defendants are the following government agencies and officers:

---

[2] The facts stated here are derived from the amended complaint and "documents incorporated into the complaint by reference," as is appropriate on a motion to dismiss. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). Plaintiffs' amended complaint incorporates, *inter alia*, the Privacy and Civil Liberties Oversight Board Report ("PCLOB Report") (July 2, 2014), the Office of the Director of National Intelligence Report ("ODNI Report") (April 22, 2015), the President's Review Group on Intelligence and Communications Technologies Report ("PRG Report") (Dec. 12, 2013), and [*Redacted*], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011).

- The NSA is headquartered in Fort Mead, Maryland, and is the federal agency responsible for conducting the surveillance alleged in this case.
- The Department of Justice is a federal agency partly responsible for directing and coordinating the activities of the intelligence community, including the NSA.
- The Office of the Director of National Intelligence is a federal agency partly responsible for directing and coordinating the activities of the intelligence community, including the NSA.
- Adm. Michael S. Rogers is the Director of the NSA and the Chief of the Central Security Service.
- James R. Clapper is the Director of National Intelligence ("DNI").
- Loretta E. Lynch is the Attorney General of the United States.

A.

Before setting forth the facts alleged in the amended complaint ("AC"), it is useful to describe briefly the statutory context pertinent to the NSA's data gathering efforts. In 1978, in response to revelations of unlawful government surveillance directed at specific United States citizens and political organizations, Congress enacted FISA to regulate government electronic surveillance within the United States for foreign intelligence purposes. FISA provides a check against abuses by placing certain types of foreign-intelligence surveillance under the supervision of the Foreign Intelligence Surveillance Court ("FISC"), which reviews government applications for surveillance in certain foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). As originally enacted, FISA required the government to obtain an individualized order from the FISC before conducting electronic surveillance in the United States. *See id.* § 1804(a). In this respect, the FISC could issue an order authorizing surveillance only if it found that there was "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2).

In 2008, thirty years after FISA's enactment, Congress passed the FISA Amendments Act, which established procedures and requirements for the authorization of surveillance targeting persons located outside the United States. *See* 50 U.S.C. §§ 1881a-1881g. Specifically, FISA Section 702, 50 U.S.C. § 1881a, "supplements pre-existing FISA authority by creating a new framework under which the [g]overnment may seek the FISC's authorization of certain foreign intelligence surveillance targeting … non-U.S. persons located abroad," *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013). Section 702 provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information"[3] if the FISC approves "a written certification" submitted by the government that attests, *inter alia*, that (i) a significant purpose of the acquisition is to obtain foreign intelligence information and (ii) the acquisition will be conducted "in a manner consistent with the [F]ourth [A]mendment" and the targeting and minimization procedures required by statute. 50 U.S.C. § 1881a(b), (g). Specifically, before approving a certification, the FISC must find that the government's targeting procedures are reasonably designed:

> (i) to ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States," *id.* § 1881a(i)(2)(B)(i);
>
> (ii) to prevent the intentional acquisition of wholly domestic communications, *id.* § 1881a(i)(2)(B)(ii);
>
> (iii) to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons

---

[3] Importantly, the statute expressly prohibits the intentional targeting of any person known at the time of acquisition to be in the United States or any U.S. person reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(b).

consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information," *id.* § 1801(h)(1); *see id.* § 1881a(i)(2)(C); and

(iv) to ensure that the procedures "are consistent with ... the [F]ourth [A]mendment," *id.* § 1881a(i)(3)(A).

In effect, an approval of government surveillance by the FISC means that the surveillance comports with the statutory requirements and the Constitution.

Additional details regarding the collection of communications under Section 702 have recently been disclosed in a number of public government reports and declassified FISC opinions. The government has disclosed, for example, that in 2011, Section 702 surveillance resulted in the retention of more than 250 million communications and that in 2014, the government targeted the communications of 92,707 individuals, groups, and organizations under a single FISC Order.[4] The total number of U.S. persons' communications that the government has intercepted or retained pursuant to Section 702 remains classified. The government has also disclosed that the NSA conducts two kinds of surveillance pursuant to Section 702. Under a surveillance program called "PRISM,"[5] U.S.-based Internet Service Providers furnish the NSA with electronic communications that contain information specified by the NSA. This case concerns the second method of surveillance, which is referred to as "Upstream surveillance."

B.

Plaintiffs challenge the NSA's use of Upstream surveillance, alleging that this mode of surveillance enables the government to collect communications as they transit the Internet

---

[4] *See* AC ¶ 37. The AC cites a redacted FISC Order and a government report for this information. *See* [*Redacted*], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011); ODNI Report, at 1, 2.

[5] "PRISM" is a government code name for a data-collection that is officially known as US-984XN. *See* PRISM/US-984XN Overview, April 2013, *available at* https://www. aclu.org/files/ natsec/nsa/20130816/PRISM%20Overview%C20Powerpoint%20Slides.pdf (last visited Oct. 22, 2015).

"backbone," the network of high-capacity cables, switches, and routers that facilitates domestic and international Internet communication. With the assistance of telecommunications providers, Upstream surveillance enables the NSA to copy and review "text-based" communications—*i.e.*, those whose content includes searchable text, such as emails, search-engine queries, and webpages—for search terms called "selectors." Importantly, selectors cannot be key words or names of targeted individuals, but must instead be specific communications identifiers, such as email addresses, phone numbers, and IP addresses.

Plaintiffs allege that Upstream surveillance encompasses the following four processes, one or more of which is implemented by telecommunications providers at the NSA's direction:

> (i) Copying: Using surveillance devices installed at key access points along the Internet backbone, the NSA intercepts and copies text-based communications flowing across certain high-capacity cables and routers.
>
> (ii) Filtering: The NSA attempts to filter the copied data and discard wholly domestic communications, while preserving international communications. Because the NSA's filtering of domestic communications is imperfect, some domestic communications are not filtered out.
>
> (iii) Content Review: The NSA reviews the copied communications that are not filtered out for instances of tasked selectors.
>
> (iv) Retention and Use: The NSA retains all communications that contain selectors associated with its targets and other communications that were bundled in transit with the targeted communications; NSA analysts may read and query the retained communications and may share the results with the FBI.

See AC ¶¶ 40, 47-49.[6]

Plaintiffs emphasize two aspects of Upstream surveillance. First, surveillance under that program is not limited to communications sent or received by the NSA's targets, as the government has acknowledged that, as part of Upstream surveillance, the NSA also engages in what is called "about surveillance"—the searching of Internet communications that are *about* its targets. AC ¶ 50. In other words, plaintiffs allege that the NSA intercepts substantial quantities of Internet traffic and examines those communications to determine whether they include references to the NSA's search terms. Second, Upstream surveillance implicates domestic communications because (i) the NSA's filters are imperfect, (ii) the NSA sometimes mistakes a domestic communication for an international one, and (iii) the NSA retains communications that happen to be bundled, while in transit, with communications that contain selectors.

---

[6] Plaintiffs' description of Upstream surveillance is based on the PCLOB Report, at 32-41.

All nine plaintiffs allege that the NSA uses Upstream surveillance to copy their Internet communications, filter the large body of collected communications in an attempt to remove wholly domestic communications, and then search the remaining communications with "selectors," looking for potentially terrorist-related foreign intelligence information. Plaintiffs further claim that these government actions invade their privacy—as well as the privacy of their staffs, Wikimedia's users, and NACDL's members—and infringe on plaintiffs' rights to control their communications and the information therein. Plaintiffs also allege that the NSA intercepts, copies, and reviews two other categories of communications specific to Wikimedia: (i) the over one trillion annual communications that plaintiffs claim occur when individuals around the globe view and edit Wikimedia websites and interact with one another on those sites; and (ii) Wikimedia's logs of online requests by such users to view its webpages. In addition to the claimed interception, copying, and selector review of their communications, plaintiffs allege that there is a "substantial likelihood" that plaintiffs' communications are retained, read, and disseminated by the NSA. *Id.* ¶ 71. This is so, plaintiffs allege, because plaintiffs, their members, and their employees communicate online with people whom the government is likely to target when conducting Upstream surveillance, and a significant amount of the information plaintiffs, their members, and their employees exchange with those persons constitutes "foreign intelligence information" under FISA. *Id.* ¶ 74. Plaintiffs further allege that Upstream surveillance undermines their ability to carry out activities crucial to their missions (i) by forcing them to take burdensome measures to minimize the risk that the confidentiality of their sensitive information will be compromised and (ii) by reducing the likelihood that individuals will share sensitive information with them.

Plaintiffs claim that the alleged injuries result from the NSA's use of Upstream surveillance that violates the First and Fourth Amendments of the Constitution and exceeds the government's authority under Section 702.[7] By way of relief, plaintiffs seek a declaration that Upstream surveillance is unlawful, an injunction prohibiting the NSA from using Upstream surveillance to intercept plaintiffs' communications, and a purge from government databases of any of plaintiffs' communications acquired through Upstream surveillance.

Defendants have moved to dismiss plaintiffs' AC pursuant to Rule 12(b)(1), Fed. R. Civ. P., on the ground that plaintiffs lack Article III standing to contest the legality of the NSA's Upstream surveillance because plaintiffs have not alleged facts that plausibly establish an actual injury attributable to the NSA's Upstream surveillance.

II.

Article III limits the jurisdiction of federal courts to certain "Cases" and "Controversies." U.S. Const. art. III, § 2, cl. 2. As the Supreme Court has made clear, one "essential and unchanging part of the case-or-controversy requirement" is that a plaintiff must establish Article III standing to sue. *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992). A plaintiff establishes Article III standing by showing that he seeks relief from an injury that is "'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper*, 133 S. Ct. at 1147 (quoting *Monsanto Co. v. Geerston Seed Farms*, 561 U.S. 139, 149 (2010)). The alleged injury must be "real and immediate," not "conjectural or hypothetical," *City of Los Angeles v. Lyons*, 461 U.S. 95, 201 (1983). The Supreme Court has "repeatedly reiterated that '[a] threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (emphases in original). Importantly, the standing inquiry is "especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional," particularly "in the fields of intelligence gathering and foreign affairs." *Clapper*, 133 S. Ct. at 1147.

---

[7] Of course, the FISC opinion that relates to the data collection practices challenged here is unavailable because it is classified. It would be helpful and generally beneficial to the public for FISC opinions to be published by way of either declassification or redaction.

Because standing is a threshold jurisdictional requirement, it may be attacked at any time, including at the outset of a case pursuant to Rule 12(b)(1), Fed. R. Civ. P. As the Fourth Circuit has made clear, where, as here, "standing is challenged on the pleadings, [a court must] accept as true all material allegations of the complaint and construe the complaint in favor of the complaining party." *David v. Alphin*, 704 F.3d 327, 333 (4th Cir. 2013) (citing *Pennell v. City of San Jose*, 485 U.S. 1, 7 (1988)). But a court should not "take account of allegations in the complaint labeled as fact but that constitute nothing more than 'legal conclusions' or 'naked assertions.'" *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). A complaint must contain "sufficient factual matter, accepted as true, to 'state a claim that is plausible on its face.'" *Ashcroft*, 556 U.S. at 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Standing is adequately alleged only if the "well-pleaded allegations" allow for a "reasonable inference," rather than a "sheer possibility," that the plaintiff has standing, *Iqbal*, 556 U.S. at 678-79; *David*, 704 F.3d at 333.[8]

III.

Clapper v. Amnesty International is the Supreme Court's most recent pronouncement on standing with respect to litigants challenging the NSA's data gathering efforts, and therefore is the leading case in this series. In *Clapper*, the plaintiffs argued that they had standing to bring a facial challenge to Section 702 because there was an "objectively reasonable likelihood" that plaintiffs' communications "[would] be intercepted" in the future. 133 S. Ct. at 1147. The Supreme Court rejected this "novel view of standing" because plaintiffs' "speculative chain of possibilities [did] not establish that injury based on future surveillance [was] certainly impending or [was] fairly traceable to [Section 702 surveillance]." *Id.* at 1146, 1150. Of course, if the alleged facts and arguments in this case are essentially identical to those in *Clapper,* then *Clapper* must control the result reached here. On the other hand, if plaintiffs in this case present facts and arguments that are different from those asserted in *Clapper*, then those facts and arguments must be carefully considered to determine whether they compel a result different from *Clapper*.

---

[8] As the parties correctly note, a jurisdictional motion to dismiss may be brought as a facial or factual challenge. *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). On a factual challenge, "a trial court may go beyond the allegations of the complaint ... [and] consider evidence by affidavit, depositions or live testimony without converting the proceeding to one for summary judgment." *Id.*; *see also Kerns v. United States*, 585 F.3d 187, 193 (4th Cir. 2009). When appropriate, a court may also grant jurisdictional discovery to ensure that the record is fully developed. *See, e.g.*, *Animators at Law, Inc. v. Capital Legal Solutions, LLC*, 786 F. Supp. 2d 1114, 1115 n.2 (E.D. Va. 2011) (granting jurisdictional discovery "to allow consideration of [a] pivotal issue on a more complete record"). Here, defendants have brought a facial challenge, but have also submitted declarations and accompanying exhibits not incorporated by reference in the complaint. As plaintiffs correctly note, this additional evidence is properly considered only if the motion to dismiss is decided on a factual—rather than facial—basis. Because the dispute can be resolved on the face of the complaint, the additional declarations and exhibits are not considered.

In the course of oral argument, plaintiffs' counsel was asked to identify the facts and arguments in this case that are different from those asserted in *Clapper*.[9] Plaintiffs' counsel identified four differences:

> (i) the legal standard in this case is different from the legal standard that controlled in *Clapper* because the standing challenge here arises on a motion to dismiss rather than, as in *Clapper*, on a motion for summary judgment.
>
> (ii) far more is known about Section 702 surveillance, including Upstream surveillance, than was known at the time of *Clapper*;
>
> (iii) the Upstream surveillance at issue here is fundamentally different from the surveillance at issue in *Clapper*; and
>
> (iv) plaintiffs here are different from the *Clapper* plaintiffs in important respects concerning their Internet communications.[10]

Clearly there are differences between the facts and arguments raised in this case and those raised in *Clapper*, but the question is not simply whether there are differences, but whether those differences compel the same or a different result from the result reached in *Clapper*.

Before addressing plaintiffs' arguments, it is important to describe *Clapper* in more detail. Plaintiffs in *Clapper* brought a facial challenge to Section 702, seeking a declaration that Section 702 was unconstitutional and an injunction against the surveillance authorized by that provision. 133 S. Ct. at 1142-46. The Supreme Court's opinion began its consideration of the standing issue by reviewing what was known and alleged concerning the NSA's surveillance practices under Section 702. Specifically, the Supreme Court explained that Section 702 surveillance "[was] subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment," emphasizing that the government must obtain the FISC's "approval of 'targeting' procedures, 'minimization' procedures, and a governmental certification regarding proposed surveillance." *Id.* at 1144, 1145 (quoting 50 U.S.C. § 1881a(a), (c)(1), (i)(2), (i)(3)). As the Supreme Court's opinion noted, "the [FISC's] role includes determining whether the [g]overnment's certification contains the required elements"[11] and whether the government's targeting procedures are "'reasonably designed' (1) to 'ensure that an acquisition ... is limited to targeting persons reasonably believed to be located outside the United States' and (2) to 'prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known ... to be located in the United States." *Id.* at 1135 (quoting 50 U.S.C. § 1881a(i)(2)(B)).

---

[9] Mot. to Dismiss Hr'g Tr. 19:13-16 (Sept. 25, 2015).

[10] *Id.* at 20:4-6, 21:12-14, 23:4-7, 27:17-21.

The Supreme Court explained that in attempting to establish standing, the *Clapper* plaintiffs did not provide "any evidence that their communications ha[d] been monitored under" any program authorized by Section 702. *Id.* at 1148. Instead, plaintiffs argued that they had standing because there was an "objectively reasonable likelihood" that plaintiffs' communications "[would] be intercepted" in the future. *Id.* at 1147. The Supreme Court's opinion characterized plaintiffs' argument as a "speculative chain of possibilities," *id.* at 1150.[12]

---

[11] As the *Clapper* majority further explained, the "[g]overnment's certification must attest" (1) that the procedures in place "'have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC]'" and "'are reasonably designed' to ensure that an acquisition is 'limited to targeting persons reasonably believed to be located outside' the United States;" (2) that the "minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons, as appropriate;" (3) that "guidelines have been adopted to ensure compliance with targeting limits and the Fourth Amendment;" and (4) that "the procedures and guidelines referred to above comport with the Fourth Amendment." *Id.* at 1145 (quoting 50 U.S.C. § 1881a(g)(2)).

[12] The speculative chain consisted of five contingencies: (i) that the "[g]overnment [would] decide to target the communications of non-U.S. persons with whom [plaintiffs] communicate;" (ii) that in targeting those communications, "the [g]overnment [would] choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance;" (iii) that "the Article III judges who serve on the [FISC would] conclude that the Government's proposed surveillance procedures satisfy [Section 702's] many safeguards and are consistent with the Fourth Amendment;" (iv) that upon such a finding by the FISC, "the Government [would]

The *Clapper* plaintiffs also argued that "they should be held to have standing because otherwise the constitutionality of [Section 702 surveillance] could not be challenged" and would be "insulate[d]" from "meaningful judicial review." The Supreme Court rejected that argument as "both legally and factually incorrect." *Id.* at 1154. The Supreme Court explained that Section 702 surveillance orders are not in fact insulated from judicial review because (i) the FISC reviews targeting and minimization procedures of Section 702 surveillance, (ii) criminal defendants prosecuted on the basis of information derived from Section 702 surveillance are given notice of that surveillance and can challenge its validity, and (iii) electronic communications service providers directed to assist the government in surveillance may challenge the directive before the FISC. *Id.* Even if these other avenues for judicial review were not available, the Supreme Court made clear that "'[t]he assumption that if [plaintiffs] have no standing to sue, no one would have standing, is not a reason to find standing.'" *Id.* (quoting *Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 489 (1982)).

In holding that plaintiffs' alleged injury was speculative, the *Clapper* majority rejected the approach advocated by the dissenting Justices. The dissent relied on "commonsense inferences" to find a "very high likelihood" that the government would "intercept at least some of" plaintiffs' communications. *Id.* at 1157 (Breyer, J., dissenting). Specifically, the dissent concluded that (i) the plaintiffs regularly engaged in the type of electronic communications that the government had "the capacity" to collect, (ii) the government was "strong[ly] motiv[ated]" to intercept for counter-terrorism purposes the type of communications in which plaintiffs engaged, and (iii) the government had in fact intercepted the same type of communications on thousands

---

succeed in intercepting the communications of plaintiffs' contacts;" and (v) that "[plaintiffs would] be parties to the particular communications that the Government intercept[ed]." *Id.* at 1148.

of occasions in the past. *Id.* at 1157-59 (Breyer, J. dissenting). The dissent also noted that the government had not "describe[d] any system for avoiding the interception of an electronic communication" to which plaintiffs were a party. *Id.* at 1159. Without evidence that a system was in place to prevent government interception of plaintiffs' communications,[13] the dissent reasoned that "we need only assume that the [g]overnment is doing its job (to find out about, and combat, terrorism) in order to conclude that there is a high probability that the [g]overnment will intercept at least some electronic communication to which at least some of the plaintiffs are parties." *Id.*

In essence, the Supreme Court held that the *Clapper* plaintiffs' chain of probabilities and inferences—based on the government's capacity and motivation to intercept communications similar to the *Clapper* plaintiffs' communications—was speculative, and therefore did not establish standing. The dissent, on the other hand, was convinced that such inferences and probabilities were sufficient to establish standing. At issue here is whether the four differences plaintiffs have identified compel the same or a different result from the result reached in *Clapper*. Each of plaintiffs' arguments with respect to those differences is separately addressed.

A.

Plaintiffs first argue that *Clapper* does not control here on the ground that the legal standard in this case is different from the legal standard applicable in *Clapper* because the standing challenge in the present case arises on a motion to dismiss rather than, as in *Clapper*, on a motion for summary judgment. To the extent this argument refers to the difference between reliance on factual allegations and reliance on a factual record, plaintiffs are undoubtedly correct.

---

[13] The majority noted that "[t]he dissent attempt[ed] to downplay the safeguards," as it "[did] not directly acknowledge that [Section 702] surveillance must comport with the Fourth Amendment … and that the [FISC] must assess whether targeting and minimization procedures are consistent with the Fourth Amendment." *Id.* at 1145 n.3.

The Supreme Court has made clear that, because the elements of standing are "an indispensable part of the plaintiff's case, each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages in litigation." *Lujan*, 504 U.S. at 561. At the summary judgment stage, a plaintiff cannot rest simply on allegations, but must "'set forth' by affidavit or other evidence 'specific facts;'" at the motion to dismiss stage, however, "allegations of injury resulting from defendant's conduct may suffice." *Id.* at 561 (quoting Rule 56(2), Fed. R. Civ. P.).

But to say the evidentiary basis is different is not to say that the standing requirements change at each successive stage. They do not. The means by which a plaintiff establishes standing—by allegation or by record evidence—changes, but the three elements of standing—actual injury, causation, and redressability—remain constant and applicable at all stages of the case. This is so because standing is a jurisdictional requirement that "is an essential and unchanging part of the case-or-controversy requirement of Article III." *Id.* at 560. Indeed, the three elements of standing are the "irreducible constitutional minimum" that "set[] apart the 'Cases' and 'Controversies' that are of the sort referred to in Article III—'serv[ing] to identify those disputes which are appropriately resolved through the judicial process." *Id.* (quoting U.S. Const. art. III, § 2, cl. 2; *Whitmore*, 495 U.S. at 155).

Thus, to withstand defendants' standing challenge on a motion to dismiss, plaintiffs must allege facts that plausibly establish (i) that there is an "injury in fact—an invasion of a legally protected interest which is concrete and particularized and actual or imminent, not conjectural or hypothetical;" (ii) that the injury is "fairly trace[able] to the challenged action of the defendant;" and (iii) that it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id.* at 560-61. A court must, of course, "accept as true all material allegations of the complaint and construe the complaint in favor of the complaining party," but a court should not "take account of allegations in the complaint labeled as fact but that constitute nothing more than 'legal conclusions' or 'naked assertions.'" *David*, 704 F.3d at 333 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). In short, a complaint alleges facts that plausibly establish standing only if the "well-pleaded allegations" allow for a "reasonable inference," rather than a "sheer possibility," that the plaintiff has satisfied each of the three elements of standing. *Iqbal*, 556 U.S. at 678-79; *David*, 704 F.3d at 333.

In sum, the standing requirement—the "irreducible constitutional minimum"—applies here just the same as it applied in *Clapper*. *Lujan*, 504 U.S. at 560. Moreover, the result in *Clapper*—that standing cannot be established on the basis of a "speculative chain of possibilities"—also applies here. 133 S. Ct. at 1150. Whether speculation is based on allegations in a complaint or facts in a record has no bearing on the outcome, as in neither context may standing be established on a "speculative chain of possibilities." *Id.*

B.

Plaintiffs next argue that *Clapper* does not control this case because more is now known about Section 702 surveillance, including Upstream surveillance, than was known at the time of *Clapper*. Plaintiffs cite in their AC several publicly disclosed documents in support of the allegation that the NSA uses Upstream surveillance to intercept substantially all international text-based Internet communications, including plaintiffs' communications.[14] Specifically, plaintiffs describe the technical features that enable the NSA to use Upstream surveillance to copy and review all or substantially all international text-based Internet communications, and the "strategic imperatives" that compel it to do so. Pls. Opp. Br. at 17. The AC alleges that:

---

[14] The AC cites, among other things, the PCLOB Report, the ODNI Report, the PRG Report, and [Redacted] , 2011 WL 10945618 (FISA Ct. Oct. 3, 2011).

> (i) the Internet backbone funnels most communications entering or leaving the United States through 49 international chokepoints, AC ¶ 46;
>
> (ii) the NSA has installed surveillance equipment at seven of those chokepoints, and the NSA has a strong incentive to intercept communications at more chokepoints in order to obtain the communications it seeks, *id.* ¶¶ 65-66, 68;
>
> (iii) the installed surveillance equipment is capable of "examin[ing] the contents of all transmissions passing through," *id.* ¶ 62 (quoting PCLOB Report, at 122);
>
> (iv) in order to identify the targeted communications, the NSA must copy and review the contents of an enormous quantity of transiting communications, *id.* ¶¶ 50, 51, 62; and
>
> (v) because the NSA cannot know in advance which Internet "packets"[15] relate to its targets, the NSA, in order to be successful, must copy and reassemble all the packets associated with international text-based communications that transit the circuits it is monitoring, *id.* ¶¶ 42, 63-64.

Plaintiffs' series of allegations does not establish Article III standing because those allegations depend on suppositions and speculation, with no basis in fact, about how the NSA implements Upstream surveillance. Specifically, plaintiffs assume that the fact that Upstream surveillance equipment has been installed at some of the Internet backbone chokepoints implies that the NSA is intercepting all communications passing through those chokepoints. That may or may not be so; plaintiffs merely speculate that it is so. Even if the NSA's surveillance equipment is capable of "examin[ing] the contents of all transmissions passing through collection devices," as plaintiffs allege, *id.* ¶ 62, it does not follow that the NSA is, in fact, using the surveillance equipment to its full potential. As with any piece of technology, technical capability is not tantamount to usage levels. For example, a car capable of speeds exceeding 200 mph is not necessarily driven at such speeds; more information is needed to conclude that the top speed is reached. And there may indeed be circumstances that suggest a limited level of use—*e.g.*, a

[15] All Internet communications are broken into "packets"—discrete chunks of information—that traverse a variety of physical circuits. AC ¶ 42. Once the packets that make up a particular communication reach their final destination, they are reassembled. *Id.*

speed limit of 70 mph. The same is true here. Plaintiffs provide no factual basis to support the allegation that the NSA is using its surveillance equipment at full throttle,[16] and the fact that all NSA surveillance practices must survive FISC review—*i.e.*, must comport with the Fourth Amendment—suggests that the NSA is not using its surveillance equipment to its full potential. In addition, plaintiffs assume that the NSA must be intercepting communications at all 49 chokepoints because the NSA has a strong incentive to do so. But apart from plaintiffs' suppositions and speculation concerning the government's incentive and decision to act in accordance with that incentive, plaintiffs provide no factual basis that the NSA is actually intercepting communications at all chokepoints.

Plaintiffs cannot provide a sufficient factual basis for their allegations because the scope and scale of Upstream surveillance remain classified, leaving plaintiffs to prop their allegation of actual injury on suppositions and speculation about how Upstream surveillance *must* operate in order to achieve the government's "stated goals." AC ¶ 64. Indeed, plaintiffs cite the government's so-called "stated goals" in nearly every facet of their argument, specifically in support of their allegations regarding: (i) the volume of communications collected by Upstream surveillance, Pls. Opp. at 22, 28; (ii) the geographic distribution of the sites at which Upstream collection occurs, *id.* at 25; and (iii) the scope of Upstream surveillance at any site where it occurs, *id.* at 23, 30. It is, of course, a "possibility" that the NSA conducts Upstream surveillance

[16] Plaintiffs' AC cites a newspaper article that claimed "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A. Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, http://nyti.ms/1E1nlsi. But the article's claim is speculative, as it is based on a publicly disclosed document that says the NSA "seeks to acquire communications about the target that are not to or from the target" but does not indicate that the NSA is *actually* acquiring vast amounts of internet communications. *Id.* Indeed, the PCLOB Report—another document on which plaintiffs rely—refers to the article's claim as "represent[ing] a misunderstanding of a more complex reality." PCLOB Report, at 119.

in the manner plaintiffs allege, but this "bare assertion[]" is unaccompanied by "factual matter" that raises it "above a speculative level," and hence does not establish standing. *Iqbal*, 556 U.S. at 681.

In sum, plaintiffs are correct that more is known about the nature and capabilities of NSA surveillance than was known at the time of *Clapper*, but no more is known about whether Upstream surveillance *actually* intercepts all or substantially all international text-based Internet communications, including plaintiffs' communications. Thus, although plaintiffs' speculative chain is shorter than was the speculative chain in *Clapper*, it is a chain of speculation nonetheless. And *Clapper* makes clear that it is not the length of the chain but the fact of speculation that is fatal. Indeed, plaintiffs' reliance on the government's capacity and motivation to collect substantially all international text-based Internet communications is precisely the sort of speculative reasoning foreclosed by *Clapper*.[17] An alleged injury that is "speculative" does not establish Article III standing, especially the standing of litigants who seek to challenge the constitutionality of government action in the field of foreign intelligence. *Clapper*, 133 S. Ct. 1147-50.[18]

---

[17] As described above, the Supreme Court in *Clapper* rejected the argument that standing could be based on a "very strong likelihood" that the NSA would "intercept at least some of plaintiffs' communications" based on speculation about the government's "motivat[ion]" to exercise its "capacity" for such interception. 133 S. Ct. at 1159 (Breyer, J., dissenting). The same line of speculative reasoning was recently rejected by the D.C. Circuit in a case involving NSA surveillance. *Klayman*, 2015 WL 5058403, at *7 (Williams, J.) (holding that the plaintiffs' standing to challenge NSA bulk collection of telephone records could not be grounded in "their assertion that NSA's collection must be comprehensive in order for the program to be most effective").

[18] *See also Klayman*, 2015 WL 5058403, at *6 (Williams, J.) (noting that, although plaintiff may plausibly show why "the effectiveness of the program [would] expand with its coverage," such a showing does not make plaintiffs' claims of actual injury any less speculative).

C.

Plaintiffs further allege that *Clapper* does not control here because newly disclosed information reveals that Upstream surveillance is fundamentally different from the surveillance at issue in *Clapper*. Specifically, Upstream surveillance involves the use of "about surveillance," which the NSA allegedly uses to review every portion of everyone's communications—a broader mode of surveillance than the targeted surveillance of particular individuals' communications that was at issue in *Clapper*. Plaintiffs contend that "about surveillance" is the "digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase." Pls. Br. at 10. This analogy is inapt; contrary to plaintiffs' contention, the publicly disclosed documents on which plaintiffs rely do not state facts that plausibly support the proposition that "about surveillance" involves examining *every* portion of *every* copied communication. According to the PCLOB Report cited by plaintiffs,

> [T]he NSA's 'upstream collection' … may require access to a larger body of international communications than those that contain a tasked selector[,] … [but] the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector.

PCLOB Report, at 111 n.476. Indeed, "[o]nly those communications … that contain a tasked selector go into government databases." *Id.* Thus, plaintiff's contention that "about surveillance" is like the hypothetical government agent reading every piece of mail misses the mark. Unlike the hypothetical government agent reading every word of every communication and retaining the information, "about surveillance" is targeted insofar as it makes use of only those communications that contain information matching the tasked selectors.

Even if plaintiffs' description of "about surveillance" were correct, it would not change the result reached here. Plaintiffs' claim of actual injury resulting from "about surveillance" rests on plaintiffs' allegation that the NSA uses Upstream surveillance to intercept substantially all international text-based Internet communications. And as already discussed, that allegation is a "bare assertion[]" unaccompanied by "factual matter" that raises it "above a speculative level." *See Iqbal*, 556 U.S. at 681; *see also Clapper*, 133 S. Ct. at 1150. Details about the tools of Upstream surveillance reveal how Upstream surveillance functions when the NSA engages in that mode of surveillance, but those details do not cure the speculative foundation on which plaintiffs' claim of actual injury is based—that the NSA is *in fact* using Upstream surveillance to intercept substantially all text-based international Internet communications, including plaintiffs' communications.

D.

Plaintiffs next argue that *Clapper* does not control here because plaintiffs are different from the *Clapper* plaintiffs in important respects concerning their Internet communications. Although six of the nine plaintiffs in this case were plaintiffs in *Clapper*, plaintiffs identify two differences related to the new parties: (i) two clients of an NACDL attorney have received notice that they are targets of Section 702 surveillance and (ii) Wikimedia engages in over one trillion communications each year that are distributed around the globe.

1. NACDL Attorney Dratel

With respect to the first difference, plaintiffs argue that they adequately allege an actual injury because the government acknowledged that NACDL attorney Joshua Dratel's client, Agron Hasbajrami, was subject to Section 702 surveillance and another Dratel client, Sabirhan Hasanoff, was prosecuted on the basis of officially acknowledged Section 702 surveillance.[19]

---

[19] *See* Letter re Supplemental Notification, *United States v. Hasbajrami*, 1:11-cr-00623, ECF No. 65 (E.D. N.Y. Feb. 24, 2014); *See* Mem. Of Law, *Hasanoff v. United States*, 10 Cr. 162 (S.D.N.Y. Feb. 11, 2015), ECF No. 208, at 10-11.

Plaintiffs allege that as a result of this government acknowledged surveillance, Dratel's own international Internet communications were *likely* intercepted and retained because he *almost certainly* communicated with or about the targeted foreign individuals in the course of representing his clients. As plaintiffs note, Dratel's scenario is similar to a hypothetical mentioned in *Clapper*, in which the government "monitors [a] target's conversations with his or her attorney." 133 S. Ct. at 1154. The Supreme Court in *Clapper* described such a scenario as likely "hav[ing] a stronger evidentiary basis for establishing standing" than the *Clapper* plaintiffs had. *Id.* at 1154.

Here, however, the facts alleged differ from the *Clapper* hypothetical in important respects. The Supreme Court in *Clapper* was describing a situation in which there was some basis for an allegation that the government had "monitor[ed a] target's conversations with his or her attorney" using the type of surveillance at issue in the case, not a situation where an attorney lacks "concrete evidence to substantiate [his] fears." *Id.* Plaintiffs in this case, by contrast, do not allege facts that plausibly establish that the information gathered from the two instances of Section 702 surveillance was the product of Upstream surveillance. In neither of Dratel's cases did the government indicate whether the information at issue was derived from PRISM or Upstream surveillance, and no factual allegations in the AC plausibly establish that Upstream surveillance—rather than PRISM—was used to collect the information. Moreover, given what is known about the two surveillance programs, it appears substantially more likely that PRISM collection was used in these cases because, according to a 2011 FISC Order, the "vast majority" of collected communications are obtained via PRISM, not Upstream surveillance. [*Redacted*], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011) (finding that "upstream collection constitute[d] only approximately 9% of the total Internet communications [then] acquired by [the] NSA under Section 702").

2. Wikimedia

Plaintiffs next allege that Wikimedia has standing because it is "virtually certain" that Upstream surveillance has intercepted at least some of Wikimedia's communications given the volume and geographic distribution of those communications. Specifically, Wikimedia allegedly engages in more than one trillion international text-based Internet communications each year and exchanges information with individuals in nearly every country on earth.

At the outset, an important implication of plaintiffs' allegation regarding Wikimedia's Internet communications must be noted. Plaintiffs have not alleged that any of the other eight plaintiffs (besides Wikimedia) engage in a substantial number of text-based international Internet communications. Indeed, plaintiffs simultaneously allege that (i) all nine plaintiffs "collectively engage in more than a trillion sensitive international [I]nternet communications each year," AC ¶ 58; and (ii) "Wikimedia engages in more than one trillion international communications each year," *id.* at ¶ 88. The AC does not quantify the other eight plaintiffs' communications. Thus, insofar as plaintiffs seek to establish standing on the basis of probabilities grounded in the volume of communications, plaintiffs' effort is limited to Wikimedia, as the AC says nothing about the volume of the other plaintiffs' communications.

With respect to Wikimedia, plaintiffs contend that Wikimedia's communications traverse all of the chokepoints at which the NSA conducts Upstream surveillance, however many that may be.[20] Plaintiffs argue that, because Upstream surveillance could achieve the government's stated goals *only if* Upstream surveillance involved the copying and review of a large percentage of internatinoal text-based Internet traffic at each chokepoint that is monitored, it is virtually certain that the government has copied and reviewed at least one of Wikimedia's communications. Specifically, plaintiffs assume a 0.00000001% chance that any particular text-based Internet communication will be copied and reviewed by the NSA to conclude that the odds of the government copying and reviewing at least one of plaintiffs' over one trillion communications in a one-year period would be greater than 99.9999999999%. AC ¶ 58. Given the large volume of Wikimedia's communications with individuals all over the world, plaintiffs claim that some of Wikimedia's communications *almost certainly* traverse every major Internet circuit connecting the United States with the rest of the world. *Id.* ¶ 61.

---

[20] The government has acknowledged using Upstream surveillance to monitor communications on more than one "international Internet link" or "circuit" on the Internet backbone. *Id.* at *15;

Plaintiffs' argument is unpersuasive, as the statistical analysis on which the argument rests is incomplete and riddled with assumptions. For one thing, plaintiffs insist that Wikimedia's over one trillion annual Internet communications is significant in volume.[21] But plaintiffs provide no context for assessing the significance of this figure. One trillion is plainly a large number, but size is always relative. For example, one trillion dollars are of enormous value, whereas one trillion grains of sand are but a small patch of beach. Here, the relevant universe for comparison purposes is the total number of annual Internet communications, a figure that plaintiffs do not provide—nor even attempt to estimate—in the AC. Without defining the universe of the total number of Internet communications, it is impossible to determine whether

---

PCLOB Report 36–37. Plaintiffs, citing a publicly disclosed NSA document, allege that the NSA has installed Upstream surveillance equipment at seven of the 49 chokepoints. *See* AC ¶ 68.

[21] AC ¶ 58 ("[T]he sheer volume of [p]laintiffs' communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of those communications.").

Wikimedia's alleged one trillion annual Internet communications is significant or just a drop in the bucket of all annual Internet communications.

Moreover, plaintiffs conclude that there is a greater than 99.9999999999% chance that the NSA has intercepted at least one of their over one trillion communications on the basis of an arbitrary assumption, namely that there is a 0.00000001% chance that the NSA will intercept any particular Internet communication. AC ¶ 58. Plaintiffs provide no basis for the 0.00000001% figure, nor do they explain why the figure is presented as a conservative assumption.[22] Plaintiffs seem to presume a string of zeros buys legitimacy. It does not. Indeed, a closer looks reveals that the number of zeros chosen by plaintiffs leads conveniently to plaintiff's desired result. If three more zeros are added to plaintiffs' figure (0.00000000001%), the odds that at least one of Wikimedia's one trillion annual communications is intercepted drops to approximately 10%. If four more zeros are added (0.000000000001%), the odds that at least one of Wikimedia's communications is intercepted drops to 1%. In short, plaintiffs' assumption appears to be the product of reverse engineering; plaintiffs first defined the conclusion they sought—virtual certainty—and then worked backwards to find a figure that would lead to that conclusion. Mathematical gymnastics of this sort do not constitute "sufficient factual matter" to support a "plausible" allegation. *Ashcroft*, 556 U.S. at 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). And contrary to plaintiffs' efforts, the "speculative" reasoning foreclosed by *Clapper* cannot be avoided by dressing "a chain of possibilities" in the clothing of mathematical certainty when the calculation lacks a statistical basis. 133 S. Ct. at 1150.[23]

---

[22] *Id.* ("*even* if one assumes a 0.00000001% chance" that "the NSA [intercepts] any particular communication") (emphasis added).

[23] Plaintiffs' probability analysis also assumes that (i) the chance of interception for each communication is the same and (ii) the interception of one communication does not affect the

Furthermore, plaintiffs' allegation that interception of Wikimedia's communications is virtually certain fails for a more fundamental reason. Logically antecedent to plaintiffs' flawed statistical analysis are plaintiffs' speculative claims about Upstream surveillance based on limited knowledge of Upstream surveillance's technical features and "strategic imperatives." Pls. Opp. Br. at 17. In other words, the "virtual certainty" plaintiffs allege assumes that the NSA is *actually* using Upstream surveillance in the way plaintiffs suppose is necessary for that mode of surveillance to achieve the NSA's stated goals. As already discussed, although plaintiffs have alleged facts that plausibly establish that the NSA uses Upstream surveillance at some number of chokepoints, they have not alleged facts that plausibly establish that the NSA is using Upstream surveillance to copy all or substantially all communications passing through those chokepoints. In this regard, plaintiffs can only speculate, which *Clapper* forecloses as a basis for standing. Indeed, the Supreme Court in *Clapper* rejected the argument that standing could be based on a "very strong likelihood" that the NSA would "intercept at least some of plaintiffs' communications" based on speculation about the government's "motivat[ion]" to exercise its "capacity" for such interception. 133 S. Ct. at 1159 (Breyer, J. dissenting). Relying on a speculative foundation regarding how Upstream surveillance must operate, plaintiffs fail to allege that an injury is "real and immediate" rather than "conjectural or hypothetical." *Lyons*, 461 U.S. at 201. This is true regardless of how probable NSA interception of Wikimedia's

---

odds of any other communication's interception. In other words, plaintiffs assume that a communication from Syria has the same likelihood of being intercepted as a communication from Canada and that the fact that a communication from a Syrian computer has been intercepted has no bearing on the likelihood that a subsequent communication sent from the same computer in Syria will be intercepted. Moreover, plaintiffs provide no evidence of how many of Wikimedia's international Internet communications are transmitted to or from areas of the world in which interception is more likely.

communications would be if the NSA were *in fact* routinely using Upstream surveillance to intercept substantial quantities of text-based Internet communications.[24]

In the end, plaintiffs' standing argument boils down to suppositions about how Upstream surveillance *must* operate in order to achieve the government's stated goals. Of course, in a case like this, plaintiffs necessarily rely on probabilities and speculation because most facts about Upstream surveillance remain classified, and hence plaintiffs see through a glass darkly. Nevertheless, the speculative reasoning plaintiffs advance is not a basis for standing under *Clapper*. *See id.* at 1147-50. To see why this must be so, consider the risks of error at play on a threshold standing question. On the one hand, a court that does not find standing on the basis of probabilities and suppositions runs the risk of a false negative—closing the courthouse doors to a plaintiff who suffers an actual injury fairly traceable to the defendant. On the other hand, a court that bases standing on such speculation runs the risk of a false positive—proceeding in a litigation that is not a "Case[]" or "Controvers[y]" under Article III. U.S. Const. art. III, § 2, cl. 2. Obviously, both risks of error should be avoided where possible, but where, as here, a court is confronted with substantial uncertainty, the risk of a false positive is of greater concern because it implicates an existential question about the litigation—whether it is, in fact, a case or controversy—and the limits of the judiciary's power in relation to the other branches of government.[25] As the Supreme Court recognized in *Clapper*, this is especially true where, as here, "reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional," particularly "in the fields of intelligence gathering and foreign affairs." *Clapper*, 133 S. Ct. at 1147. Thus, as *Clapper* dictates, standing cannot be established on the basis of mere speculation. *See id.* at 1147-50. Accordingly, plaintiffs in this case lack standing on that ground to challenge the NSA's use of Upstream surveillance.[26]

---

[24] Plaintiffs also cite a publicly disclosed NSA document, which states that "HTTP" is used in "nearly everything a typical user does on the Internet" and identifies Wikipedia (along with several other well-known websites) as an example of a source of HTTP communications. AC ¶ 107. But as defendants correctly point out, the document does not help to establish an injury to Wikimedia that is fairly traceable to Upstream surveillance because it neither identifies Upstream surveillance nor gives any indication that the NSA is actually collecting the communications of the websites listed.

IV.

Plaintiffs further allege actual injury on the ground that Upstream surveillance undermines plaintiffs' ability to carry out activities crucial to their missions (i) by forcing them to take burdensome measures to minimize the chance that the confidentiality of their sensitive information will be compromised and (ii) by reducing the likelihood that individuals will share sensitive information with them. Attorney Dratel, for example, allegedly employed burdensome electronic security measures to protect his communications with his clients and, in some instances, travelled abroad to gather information in person.

The *Clapper* plaintiffs advanced indistinguishable arguments, and the Supreme Court flatly rejected them, explaining that the alleged injuries were not "fairly traceable to [Section

---

[25] *See Lujan*, 504 U.S. at 559-60 ("[T]he Constitution's central mechanism of separation of powers depends largely upon common understanding of what activities are appropriate to legislature, to executives, and to courts," which includes identifying cases "that are of the justiciable sort referred to in Article III").

[26] In addition to alleging that some of their communications are intercepted, plaintiffs allege a "substantial likelihood" that some of those communications must be retained, read, and disseminated by the NSA. AC ¶ 71. This allegation necessarily fails. Because plaintiffs have not plausibly alleged initial NSA interception of their text-based Internet communications, it follows that they have not adequately alleged that any of their communications are retained, read, or disseminated by the NSA.

702]" because (i) plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending" and (ii) plaintiffs cannot establish injury "based on third parties' subjective fear of surveillance." 133 S. Ct. at 1151, 1152 n.7.[27] Thus, *Clapper* controls here. The subjective fears of third parties and any alleged burdensome measures taken as a result of subjective fear of surveillance are not fairly traceable to Upstream surveillance, and therefore do not establish Article III standing.

V.

A final point, raised in *Clapper*, merits mention here: whether the standing requirement as applied in *Clapper* bids fair to immunize Section 702 and Upstream surveillance from judicial scrutiny. This concern is misplaced. To be sure, no government surveillance program should be immunized from judicial scrutiny, and indeed Section 702 and Upstream surveillance have no such immunity. As the *Clapper* majority noted, Section 702 surveillance is reviewed when: (i) the FISC reviews targeting and minimization procedures of general surveillance practices to ensure, *inter alia*, "the targeting and minimization procedures comport with the Fourth Amendment," (ii) criminal defendants prosecuted on the basis of Section 702 surveillance challenge the validity of that surveillance, and (iii) electronic communications service providers who are directed to assist the government in surveillance challenge the directives before the FISC. *Clapper*, 133 S. Ct. at 1154. Moreover, the recently enacted USA FREEDOM Act provides that amicus curiae may be appointed to represent the public in certain FISC proceedings involving NSA surveillance pursuant to Section 702. Pub. L. No. 114-23, 129 Stat. 268, 279.[28] These examples, of course, are not civil challenges to Section 702, and establishing standing to challenge Section 702 in a civil case is plainly difficult. But such difficulty comes with the territory. It is not a flaw of a classified program that standing to challenge that program is not easily established; it is a constitutional requirement essential to separation of powers.

---

[27] The amici curiae in this case argue that standing can be established on the ground that the alleged government surveillance chills speech protected by the First Amendment. *See* Br. of *Amici Curiae* American Booksellers Association, *et al.*, at 12-17; Br. of *Amici Curiae* First Amendment Scholars, at 9-19. As with plaintiffs' argument, the amici curiae's argument fails for the reasons articulated in *Clapper*. 133 S. Ct. at 1150-52. Both amicus briefs, which focus chiefly on the chilling argument, have been carefully reviewed and found unpersuasive. It is also worth noting that the only other nine individuals who cite their own works as frequently as do the nine authors of the First Amendment Scholars amicus brief are members of the Supreme Court, who, unlike the amici, do so out of sheer necessity.

VI.

For the reasons stated here, defendants' motion to dismiss is granted.

An appropriate Order will issue.

Alexandria, Virginia
October 23, 2015

/s/
T. S. Ellis, III
United States District Judge

[28] It should also be remembered that the classified program at issue here is authorized by a law that was passed through the democratic process. Should society's suspicions about surveillance programs rise to a level sufficient to cause citizens to suspect Orwellian harms that outweigh the benefits to national security, surveillance programs can be revised or eliminated the same way they were authorized, namely through the legislative process. It is also possible that the jurisprudence of constitutional standing may change in the future.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION, *et al.*,	)	
Plaintiffs,	)	
	)	
v.	)	**Case No. 1:15-cv-662**
	)	
NATIONAL SECURITY AGENCY /	)	
CENTRAL SECURITY SERVICE, *et al.*,	)	
Defendants.	)	

ORDER

This matter came before the Court on defendants' Motion to Dismiss for lack of jurisdiction pursuant to Rule 12(b)(1), Fed. R. Civ. P (Doc. 77). The matter was fully briefed and argued.

For good cause, and for the reasons stated in the Memorandum Opinion,

It is hereby **ORDERED** that defendants' Motion to Dismiss is **GRANTED**.

The Clerk is directed to send a copy of this Order to all counsel of records and to place this matter among the ended causes.

Alexandria, Virginia
October 23, 2015

/s/
T. S. Ellis, III
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *et al.*, *Plaintiffs*, v. NATIONAL SECURITY AGENCY, *et al.*, *Defendants*.	Hon. T.S. Ellis, III Civil Action No. 15-cv-00662-TSE

NOTICE OF APPEAL

All Plaintiffs in the above-captioned case hereby appeal to the United States Court of Appeals for the Fourth Circuit from the final order entered in this action on the 23rd day of October, 2015, granting Defendants' motion to dismiss for lack of jurisdiction.

_______________*/s/*_______________
Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

_______________*/s/*_______________
Patrick Toomey (pro hac vice)
(*signed by Patrick Toomey with permission of Deborah A. Jeon*)
Jameel Jaffer (pro hac vice)
Alex Abdo (pro hac vice)
Ashley Gorski (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Charles S. Sims (pro hac vice)
David A. Munkittrick (pro hac vice)
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900
csims@proskauer.com

Dated: December 15, 2015

Counsel for Plaintiffs